MODERN
Defense In-Depth

A Briefing on Cybersecurity in the Era of Cloud

Safeguard Your Business through
Security Of the Cloud, On the Cloud, and Across Clouds

ORACLE

Building Smarter Cloud Security Systems

It’s easy to think of cybersecurity as a simple arms race: We build higher walls; hackers build taller ladders.

But the reality is far more complex. There are many ways hackers can gain access to a system, and they’re continually trying to exploit every single one. As such, **your security is only as strong as the weakest link**. The solution isn’t just a taller wall. It’s a wall, a moat, a ring of barbed wire, land mines, booby traps…

You get the idea. Keeping data safe — in the cloud and anywhere online — **requires defense in-depth**. The threat footprint spans users, networks, applications, servers, and hardware. That’s true whether they’re on controlled premises, or in public clouds.

In this briefing, we’ll build a case for an in-depth modern defense that protects your business everywhere it runs, limiting risks posed by bad actors, malicious insiders, and tenants of public clouds.

Use this expert advice to strengthen your cloud security and protect your customers, your data, and your business.

Contents

BRIEFING ONE: EXTERNAL THREATS

BRIEFING TWO: INTERNAL THREATS

BRIEFING THREE: RISKS TO HARDWARE AND SUPPLY CHAIN

BRIEFING FOUR: THE CROSS-TENANT THREAT

BRIEFING FIVE: PUTTING IT ALL TOGETHER

BRIEFING SIX: VENDOR SOLUTIONS

BRIEFING ONE

External Threats

Cybercrime has become big business, with thousands of participants in this new illegal economy. Hackers ranging from amateurs to sophisticated nation-states use troves of available tools, collaborating to probe for vulnerabilities, distribute malicious software, and mine it for data or ransom.

$8 Trillion

Data breaches will cost businesses $8 Trillion between 2017 and 2022.*

*Juniper Research

EXTERNAL THREATS

Threat Profiles

Data theft from malicious outsiders has become common headline news. These attacks result in theft of personally identifying information including contact details, social security numbers, health histories, and credit cards. Organizations of all types, and businesses of every size and industry, have fallen victim. These attacks have become so inexpensive and easy to carry out that hackers are taking aim at every site on the internet, leveraging automated attack tools.

Hackers hijack legitimate devices and use them as part of a network — or "botnet" — to launch unwanted traffic at web sites, distribute malware, and exfiltrate or steal information from victim devices and websites. Examples of bot and botnet attacks include:

DISTRIBUTED DENIAL OF SERVICE

Bots flood a website with fake traffic, overloading system resources. This causes outages, blocking legitimate traffic from getting through.

INFILTRATION

Bots constantly probe websites for vulnerabilities like default passwords and out-of-date software.

DATA BREACH

When bots discover a vulnerability, they can leverage it to expose data, erase it, or make it unavailable until a ransom is paid.

EXTERNAL THREATS

Layers of Security

External attacks vary in method and aims. As such, they require an equally sophisticated defense strategy. Make sure to include these components:

✓ DDOS ATTACK PROTECTION

Software can detect an incoming surge of malicious traffic and deflect it from your site using a globally distributed network of scrubbing centers.

✓ BOT MANAGEMENT & MITIGATION

Cloud-native intelligent tools can assess incoming traffic to determine whether it is legitimate or malicious, blocking the latter.

✓ WEB APPLICATION SECURITY

Use of advanced methods including machine learning can flag attempts to steal data and prevent it from leaving a protected resource or perimeter.

✓ MANAGED DNS

A managed domain naming service keeps tracking of malicious sites and blocks connection to them.

✓ CREDENTIAL CONTROLS

Software can help control what level of access individual users have and deactivate stolen credentials.

✓ ENDPOINT DEVICE PROTECTION

Protection software can help prevent malicious attacks on individual user devices, detecting attempts to install malicious code and blocking infection.

✓ IDENTITY MANAGEMENT

Identity and access management (IAM) solutions help keep bad actors from impersonating legitimate users and gaining unauthorized access. These tools capture and record login attempts, manage user identities, and facilitate authorization and removal of privileges.

> "
>
> In our recent Cloud Threat Report, we asked respondents how concerned they were with 13 different types of threats over the next 12 months. All 13 different types of attacks had at least half of all respondents highly concerned. That shows that external threats are highly varied, damaging, and keeping security experts awake at night.
>
> **LAURENT GIL**
> Product Strategy Architect at Oracle Cloud Infrastructure

EXPERT ADVICE

Make Security an Ongoing Concern

RICH TEHRANI
Futurist & Corporate Advisor, CEO at TMC
@rtehrani

“Online cyber safety is a constant struggle. Sadly, there is no single way to protect from all potential cyber threats. Eventually, every system can be compromised. But the most vigilant IT managers, CSOs, and CTOs will be safest.

You should work with specialized service providers or content delivery networks (CDNs) to deal with DDoS attacks. In addition, all companies must have cybersecurity training, auditing and system documentation, anomaly detection, pen testing, and phishing simulation exercises. Obviously, antivirus solutions need to be up-to-date — likewise with patches.

Companies need to evaluate what data is at risk, ensuring it is encrypted at rest, in movement, and in use. At the end of the day, companies must have a cybersecurity culture. They need to have multiple sets of eyes reviewing systems and procedures in the hopes that hackers will look for an easier target, and to ensure each team member knows what their role is in the process.”

“Companies must have a #cybersecurity culture. They have to have multiple sets of eyes reviewing systems and procedures.” @rtehrani

Click to Tweet

EXPERT ADVICE

Use Bot Management to Classify Traffic & Neutralize Threats

LAURENT GIL
Product Strategy Architect at Oracle Cloud Infrastructure
@laurentgil

"Bot management is a feature of an application security platform that identifies whether the requests that come into a website or to a mobile application are coming from a human or a machine.

Now, there are some machines that are fine, like Google's bots. You obviously want Google bots to access your pages. But you don't want other bots — malicious bots or unknown bots — trying to gain access.

Our task is to classify incoming requests as 'human' or 'good bot.' And anything that is not a good bot would be classified as a 'malicious bot' or 'unknown.' However, in our world, 'unknown' is the same as 'malicious.' You can't afford to assume something unknown has good intent.

That's the first step. Now, even if the traffic is a good bot or a human, that doesn't mean it's completely safe. That is what a web application firewall would evaluate. So bot management is just one layer of applications security, which must be part of a bigger platform."

> *"In #cybersecurity, 'unknown' is the same as 'malicious.' You can't afford to assume unknown traffic has good intent."*
> *@laurentgil*
>
> *Click to Tweet*

BRIEFING TWO

Internal Threats

When you think of an internal attack, don’t imagine a traitorous employee stealing data. Internal threats typically originate with malicious insiders or credential theft and device takeover, making a well-meaning insider an unwitting accomplice.

Four percent of people will click on any given phishing campaign. If your organization has 1,000 employees, that’s 40 opportunities for hackers to steal credentials.*

* Verizon

INTERNAL THREATS

Threat Profiles

While there are data theft incidents that are perpetrated by malicious insiders, the more common scenario is a device infected with malware, which then allows the attacker to access the privileged insider's credentials. The prevalence of attacks and data theft from stolen credentials requires that we constantly monitor users' levels of access and privilege.

Here are a few of the most common types of attack:

SOCIAL ENGINEERING/PHISHING

Hackers ask for sensitive information over the phone or email, posing as trusted individuals. 78% of cyber espionage incidents in 2018 involved phishing.*

UNAUTHORIZED DEVICES

Your company laptops may be locked down tight, but what about your employees' personal smartphones? Laptops, tablets, anything with an IP address can be a launching point for an attack.

UNAPPROVED APPLICATIONS

In large companies, some departments might bypass the IT department and create their own solutions. Use of applications and services that do not have the benefit of IT oversight can be a major source of risk.

*Verizon

INTERNAL THREATS

Internal Layers of Defense

To most effectively safeguard against internal threats, you need a combination of training, creating a culture of security, and technological solutions.

ENCRYPTION

Default encryption for all data at rest can prevent data misuse even in the event of theft.

SECURITY TRAINING

Create a culture of security with employee training. Educate on social engineering attacks, password hygiene, and device best practices, including your Shared Responsibility Security Model.

DNS SECURITY EXTENSIONS (DNSSEC)

DNSSEC adds additional signatures to the data that comes through your DNS, ensuring data integrity.

ACCESS CONTROL & AUTHENTICATION

Use a standardized Identity Access Management solution to set permissions and manage access, authentication, and behavior monitoring/response. Enforce least privileged access for all, including administrative personnel, and monitor the use of those privileges to ensure it is business and mission appropriate. Anomalies should be investigated for possible insider threat.

EXPERT ADVICE

Strengthen Your First Line of Defense

MICHAEL FISHER
Systems Analyst, Whitcraft Group
@fisher85M

in

"To assist with social engineering attacks, one thing we need to recognize is that the first line of defense is the users themselves. To help mitigate social engineering attacks, employees should be trained on a regular basis about the risks so they know when to raise their hand. Processes and procedures for company visitors can help eliminate some of the low-hanging fruit of social engineering attacks. Having good IT governance in place will help with the overall effort, but what it really comes down to is the training and processes."

"To help mitigate social engineering attacks, employees should be trained on a regular basis to know the risks." @fisher85M.

Click to Tweet

EXPERT ADVICE

Guard Against Phishing and Email Compromise

GREG JENSEN
Senior Director of Cloud Security, Oracle
@GregJensen10

"Phishing attacks and email compromises are extremely common tactics for attackers looking to gain access to your systems. Fortunately, these can be mitigated with great success by incorporating a combination of traffic analysis and multi-factor authentication (MFA).

A commercial traffic analysis solution can perform sophisticated analysis of your inbound email stream, working to weed out suspicious emails before they reach your end users. Should an attacker succeed in prompting a user to disclose their corporate credentials, modern identity management controls can kick in to force secondary forms of authentication that only the legitimate account owner would know — known as multi-factor authentication (MFA).

An additional way to mitigate risk is to use a URL reputation service. These analyze the embedded URLs found within emails or documents and strip away or flag malicious URL insertions which, when clicked on, lead users to infected or fake web sites.

The key to success here is based around people, process, and technology. In addition to the technologies noted above, it is critical to focus on continued training of all employees to help identify the signs of a phishing attack, and the processes to report and respond to these attacks.

Employees should learn to recognize attacker methods and illegitimate requests for privileged information. Internally conducted phishing campaigns can also help identify how well awareness training is working and which employee populations are more vulnerable and in need of supplemental training."

"It is critical to focus on continued training of all employees to help identify the signs of a phishing attack, and the process to report and respond to these attacks." @GregJensen10

Click to Tweet

EXPERT ADVICE

Increase Protection with Constant Authentication

RATAN JYOTI
Chief Information Security Officer,
Ujjivan Small Finance Bank Limited
@reach2ratan

"Continuous Authentication is the need of the hour. Once a user is successfully authenticated based on their credentials or biometry, a continuous authentication system should monitor the user's behavior on their endpoints and workstations to rule out account takeover. This system can continuously authenticate users as need be and keep balance between user experience and security. Many times, authentication can be automated at all access points."

> *"Continuous authentication is the need of the hour. Once a user is successfully authenticated, a continuous authentication system should monitor to rule out account takeover." @reach2ratan*

Click to Tweet

BRIEFING THREE

Risks to Hardware and Supply Chain

Supply chain security is an ever-increasing area of concern. In particular, hardware can be infected with malware somewhere between the manufacture and delivery to an end user. These types of attacks require skill to carry out, but can be very hard to spot.

80%

It’s estimated that 80% of cyber breaches start in the supply chain.*

*Industry Week

RISKS TO HARDWARE AND SUPPLY CHAIN

Threat Profile & Security Solutions

THREAT PROFILE

Some of the most insidious attacks happen deep within infrastructure hardware. Vulnerabilities can be introduced to servers at the firmware level. These attacks can be carried out via supply chain attack and through third-party suppliers. This year, researchers discovered firmware vulnerabilities in servers used by multiple brands, designed to hide malware before the server even had an operating system installed.*

Malware can be loaded through code insertions into the device's firmware, lurking in extensions added to operating systems, even tucked away in storage systems. Once the vulnerability is introduced, it can spread from servers to networks and beyond.

LAYERS OF DEFENSE

Businesses need to know that their hardware is trustworthy down to the BIOS. Since most businesses are using a combination of cloud and local storage, that means finding trusted vendors for both. In the cloud where customers are reliant on the cloud service provider to deliver pristine hardware, it is important to understand whether the cloud service provider has a process for ensuring that hosts are free of malware.

*Computer Weekly

EXPERT ADVICE

Create a Baseline to Identify Abnormal Behavior

KEN WESTIN
Director, ITOA & Security Solutions, Elastic
@kwestin

“The cyberthreats organizations face today are very different from the threats faced even just a few years ago, however defenses are still generally focused on known threats and external threat intelligence. When we are looking at root-level threats at the hardware level, we are dealing with either supply chain compromises, software/ firmware tampering, or a more advanced adversary in general. It is with this in mind that we cannot rely on boundary defenses or blocking known threats. We need to be looking at what is “normal” in our environment and baseline that behavior. From there we can identify anomalies and be able to investigate them in more depth.

The challenge with this is that organizations need to gather the appropriate telemetry from INSIDE their network. This usually involves collection of wire data from the network, as well as more verbose logging on the endpoint using either commercial tools or a wide range of open source tools that are available. This data then needs to be aggregated and stored in a flexible platform that can be used for analysts to leverage more advanced analytics tools including machine learning to help identify and baseline behavior, as well as pivot to investigate these threats further. For example, beaconing activity from a root-level attack may look innocuous, but if it is using an odd protocol such as DNS and at odd times? What do the packets look like? Is this normal for this category of asset? Then being able to pivot to the endpoint to identify what processes are being spun up on that device: Are these normal? Have we seen them before?”

“We cannot rely on boundary defenses or known threats. We need to be looking at what is normal in our environment, baseline that behavior, and identify anomalies from there.” @kwestin #cybersecurity

Click to Tweet

BRIEFING FOUR

The Cross-Tenant Threat

A major concern of cloud tenants is whether a neighbor’s risky behavior can expose them through the shared infrastructure.

Only 8.1% of the 20,000 cloud services in use today meet industry best practices for enterprise-grade security.*

*SkyHigh

THE CROSS-TENANT THREAT

Threat Profile & Security Solutions

THREAT PROFILE

Businesses are increasingly shifting their operation-critical data to the cloud. That makes sense: Complex business operations require the immense processing power of cloud servers. But being in the cloud means sharing hardware with other organizations. In 1st-generation cloud infrastructure — the kind most common today — threats can pass laterally between tenants on the cloud network if the attacker successfully breaches the hypervisor (i.e. the layer that makes it possible for multiple tenants to share the same hardware). That means someone else's breach can become your problem.

LAYERS OF DEFENSE

2nd-generation cloud providers significantly reduce this threat by design with isolated network virtualization, an infrastructure that logically and physically separates each tenant from its neighbors by using a dedicated hardware software layer to control traffic movement between tenants. This introduces a base layer of defense to stop unauthorized code from spreading through sites sharing the same cloud servers.

Make sure your cloud provider has this 2nd-generation capability. Isolated network virtualization is the foundation for advanced security capabilities in encryption, key management, governance, and more.

EXPERT ADVICE

Segment and Isolate on and off Cloud

ERIC VANDERBURG
Vice President, Cybersecurity, TCDI
@evanderburg

"One of the most frequently overlooked layers of security is segmentation. The business environment is increasingly connected, but some restrictions need to be in place to protect sensitive data or private information from being disclosed. Companies should allocate segments for different data types and communication streams, to separate customers, and to isolate riskier actions from the rest of the network.

Segmentation should be implemented in virtual networks, across clouds, and in many other areas outside of physical networking. For example, credit card processing systems should be isolated from other systems as part of PCI; backup archives should be isolated from production systems to prevent ransomware from affecting both; and communication streams in multi-tenant environments that traverse networks such as virtual networks over physical networks, or communication to and from containers, should be isolated per customer."

"Companies should allocate segments for different data types and communication streams, to separate customers and isolate riskier actions from the rest of the network." @evanderburg #cybersecurity

Click to Tweet

BRIEFING FIVE

Putting It All Together

You’ve seen how modern cloud security requires a complex solution set for multiple types of threats. In this section, we’ll show what a more robust cloud security model looks like.

60%

Through 2020, public cloud infrastructure will suffer 60% fewer security incidents than traditional data centers.*

*Gartner Cloud Strategy Leadership, David Mitchell Smith, 2017

PUTTING IT ALL TOGETHER

A Multi-Layered Cloud Security Model

Hackers are constantly searching for the weak link in your security armor.

As such, a multi-layered threat model must consider all threats as equally dangerous. To make sure your data is well-protected, you need a security-first system with multiple layers of defense.

A more secure cloud starts with trusted hardware, to ensure security down to the BIOS. The infrastructure built on that foundation should include network virtualization that reduces the risk to tenants from other tenants of the cloud, data is encrypted by default both at rest and in transit and security controls are available that enforce least privilege access and restrict traffic to warranted paths and access patterns.

A security-first cloud should be the trusted foundation for your new threat protection model. Cloud infrastructure providers roll out best practices at scale, develop and hone incident responses, and hire the best available security talent.

EXPERT ADVICE

Make Authentication More Usable to Promote Adoption

HELEN YU
Founder & CEO, Tigon Advisory Corp
@yuhelenyu

"There are a variety of software and process solutions that businesses can use to control and monitor access to data while keeping it available to authorized users, including identity management.

An Identity and Access Management (IAM) solution provides a multitude of supported authentication methods that allow users to select the right kind of identity verification while ensuring secured actions."

"Businesses need to have an eye for design in order to build great usability without compromising security." @yuhelenyu

Click to Tweet

EXPERT ADVICE

Control Access with a Hybrid Identity Management Platform

GREG JENSEN
Senior Director of Cloud Security, Oracle
@GregJensen10

in

"The role of identity management platforms has changed over the years, from an auxiliary component of the helpdesk to a central component of today's security identification and response program. At the center of all events, alerts and remediation efforts is a robust identity platform to help manage user and session permissions.

As we expand more business-critical workloads into the cloud, we are seeing the challenge for organizations to effectively manage these entitlements and lifecycles in a consistent way, and to provide complete governance end-to-end. Organizations have rapidly responded with new requirements that centralize these identity and access controls. The goal is to ensure unified policies are leveraged across users, data, apps, and infrastructure. That way, entitlements follow the user, no matter where they access services from.

The key to a modern identity system is rapid on-boarding of new users, devices, and applications as well as rapid deprovisioning when role or job status changes. The ability to immediately change user entitlements to applications and services, combined with the ability to ensure users are not over-entitled, is a key benefit for organizations impacted by regulatory compliance mandates.

The right identity platform should offer monitoring and entitlement management that can spot anomalies in the use of credentials — that is, credentials used out of time sequence, logging on in multiple locations at once, or simply logging on outside of normal use patterns.

Organizations that lead with a strong hybrid-identity platform will find not only decreases in costs associated with onboarding and remediation, but increases in the organizational capabilities to defend against fraud, mis-use, and loss of business-critical data."

"The key to a modern identity system is rapid on-boarding of new users, devices and applications as well as rapid deprovisioning when roles or job status changes." @GregJensen10

Click to Tweet

EXPERT ADVICE

Practice Security First and By Design

TONY FLATH
Enterprise Account Executive, Shaw Business
@TmanSpeaks

“Take a security-first and secure-by-design approach. Have a defined security policy and governance controls: NIST offer a great framework to reference.

Plan regular vulnerability and pen tests to ensure concerns are identified and remedied on a regular basis. For applications both on premise and SaaS, check with vendors and ensure adequate security controls and certifications exist.

Ongoing training and simulation is key for all employees. Forge forward with emerging technology, but take a security-first approach, with training and awareness continually reinforced.

Take a serious look at cybersecurity resources and outsource managed security where it makes sense to do so.”

> ***“Forge forward with emerging technology, but take a security first approach with training and awareness continually reinforced.” @TmanSpeaks***
>
> *Click to Tweet*

BRIEFING SIX

Vendor Solutions

Keeping your business secure is an ongoing commitment. But you don't have to go it alone. The right vendors can help provide the layers of security you need, while reducing your own IT overhead.

72%

of those surveyed said they found public cloud services to be MORE SECURE than what they can provide in their own data centers.*

*Oracle and KPMG Cloud Threat Report 2019

VENDOR SOLUTIONS

Best of Breed in a Hybrid World

We've talked a lot about cloud security so far. The cloud is a big part of the security landscape, but it's not the only one. Less than 10% of enterprise processing actually happens in the cloud today. The rest is in proprietary data centers. The most robust security solution should consolidate management of on- and off-premise data.

Because the cloud is distributed, elastically scalable, and more open, it's the best place to centralize to enhance both on-premise and cloud offerings to your business' best advantage.

COMMON CONTROL PLANE

Use the cloud to standardize control of your security policies and eliminate redundancy.

COMMON DATA PLANE

Bring data together into fewer visualization and analytics tools to more effectively receive actionable intelligence on real-time threats to sensitive data and services.

COMMON AUTOMATION OF ANALYSIS

Use cloud processing to synergize information, put machine learning to work analyzing data, and make more informed decisions.

VENDOR SOLUTIONS

Layered Defenses: Of the Cloud, On the Cloud, and Across Clouds

The current threat landscape is very challenging. Attacks are increasing in volume and complexity, and there's a shortage of workers with the skills needed to help turn the tide.

To stay ahead, businesses need layers of security. The cloud offers the easiest path to deploying these layers with speed and ease.

Companies are adopting cloud for its superior, hardened architecture and on-cloud controls that span network, data, application, and user.

Use the expert advice in this book to strengthen your layers of security now, and drive a new commitment to constant vigilance.

ORACLE

Oracle has developed a second-generation cloud built on security-first principles to protect critical enterprise workloads.

We invest resources to continuously innovate and make available security controls that our tenants can use to manage their security posture. Let us show you how to benefit from the protections we have built in the cloud, which provide protection for data and applications running on the cloud, across third party clouds, and on-premises to secure today’s modern enterprise.

Contact Oracle Now