INTRODUCTION

The face of cloud security is changing in response to morphing attack methods.

To keep your organization and your data safe, it is crucial to consider forward-thinking approaches to cybersecurity.

In this e-book, we discuss how you can augment your existing infrastructure within the data center with security measures in the cloud for a more robust web security posture. We also share Akamai’s approach to cloud security as well as those of other vendors. We then take a closer look at some commonly used, but sometimes misleading, metrics – so you can make more educated decisions about the best solutions for your needs.

TOPICS WE’LL COVER IN THIS E-BOOK:

» Why cloud-based security matters

» What scale is and how to measure it

» How even average DDoS attacks can challenge weaker solutions

» What is collective intelligence and how can it boost your preparedness

» False positives vs. false negatives: The inside story on Web Application Firewall (WAF) accuracy numbers

» How fast is fast: Looking behind the curtain to find out

» The Security Operations Center (SOC): The who, what, where, when and how of evaluating vendor claims

» Defense in depth: Implementing a multi-layered cloud security solution
WHY CLOUD-BASED SECURITY MATTERS
For the best and most secure Internet experience, enterprise organizations increasingly rely on the cloud. Why? **TWO KEY DRIVERS ARE:**

- A changing threat landscape is driving the need for more scale, accuracy, experience, and collective intelligence
- There are inherent limits with on-premises mitigation appliances and enterprise data centers for Distributed Denial-of-Service (DDoS) and web attack protection

The need for scale is the easiest to understand and can be illustrated with just a few stats.

**HOW MUCH ATTACK BANDWIDTH CAN YOU HANDLE?**

One of the largest DDoS attacks Akamai has mitigated on behalf of a single customer peaked at 623 Gigabits per second (Gbps). While unusual, it certainly was not an isolated attack. We have also mitigated attacks of 530 Gbps, 363 Gbps, 321 Gbps, 309 Gbps, and 289 Gbps. Moreover, in Q1 2016 and Q3 2016 we mitigated a record 19 mega attacks – attacks exceeding 100 Gbps.

Few enterprise organizations can defend against an attack of this magnitude. Most data centers simply do not have enough network bandwidth to absorb even an average attack.

**UNDERSTANDING ATTACK SIZES**

Attack sizes are a great data point you can use to gauge a vendor’s attack-fighting capability. However, it pays to be skeptical when vendors talk about attack sizes. In many cases, when vendors discuss large attacks, these were attacks seen but not actually mitigated or attacks that were mitigated by the vendor’s upstream providers, leaving a much smaller attack to be mitigated by the vendor itself. Always ask a vendor to see the traffic charts showing the actual attack size mitigated on their platform.

The 623 Gbps attack, for example, was a real attack Akamai stopped on our platform and our network. It is also worth noting this was part of a sustained campaign – with 10 attacks during a seven-day period. Three of these attacks exceeded 200 Gbps and two exceeded 50 Million packets per second (Mpps).

While only a few organizations are hit by such large attacks, you should at least consider the average attack size while planning your defenses. The average-sized DDoS attack observed in 2016 was just over 5 Gbps.

Even if your DDoS mitigation appliance proclaims 100+ Gbps throughput per appliance, it is probably not enough. An average-sized 5 Gbps DDoS attack can quickly overwhelm most network pipes, rendering any appliance-based solutions inside your data center useless.

Moreover, repeat attacks have become the norm. In Q3 2016, attackers targeted the same organization an average of 30 times. Furthermore, the most targeted company was hit with 427 attacks – averaging nearly five attacks per day.
UNDERSTANDING SCALE
Today’s threat landscape is driving scalability requirements and, consequently, adoption of cloud-based security solutions. However, it can be difficult to determine how much scale is enough.

**START WITH TOP-LINE NUMBERS**

A good place to start is with a vendor’s top-line capacity number. Figure 1 shows how stated capacity compares for eight solutions from six vendors. For example, Vendor 5 claims 13 Terabits per second (Tbps) for their CDN-based solution, but considerable capacity for their DDoS scrubbing solution. How much capacity is considerable?

**UNDERSTAND AVAILABLE CAPACITY**

Many vendors state their top-line capacity exceeds the largest triple-digit DDoS attacks, implying they have enough scale – but this is not necessarily true. You need to go beyond a vendor’s top-line capacity number to really understand if they can scale when you need them.

First, there is a difference in how capacity is used between Content Delivery Network (CDN)-based solutions and DDoS scrubbing solutions. In Figure 1, Vendors 1, 2, and 4 provide DDoS scrubbing solutions, whereas Vendor 3 is a CDN-based solution. Vendor 5 and Akamai offer both DDoS scrubbing and CDN-based solutions.

**THE DIFFERENCE BETWEEN CDN S AND DDoS SCRUBBING SOLUTIONS**

CDN-based solutions are always on, which means that most of their capacity is already consumed by legitimate application traffic. On the other hand, DDoS scrubbing solutions tend to be more on-demand, with more capacity available for absorbing DDoS attacks at any point in time. This distinction is important in determining how much available capacity a vendor actually has to absorb a large DDoS attack.
A CLOSER LOOK AT CAPACITY WITH CDNs

Figure 2 shows an example of a CDN-based service with 1 Tbps of claimed network capacity. As shown in Figure 1, this stated capacity is typical.

Because it is a CDN-based service, most of the capacity will already be consumed by legitimate traffic.

Let us assume your typical, multi-tenant CDN is 90% utilized. That means, of the 1 Tbps total claimed network capacity, 900 Gbps is already consumed by existing traffic. That leaves only 100 Gbps of capacity to absorb DDoS attacks. Moreover, as traffic spikes for other properties on the CDN – legitimate or malicious – the available capacity to fight attacks can deteriorate further.

When considering vendors, it is important to determine actual available capacity and whether the service will truly be able to protect you when needed.

FIGURE 2: A better measure of capacity is available capacity – the capacity the vendor has beyond legitimate traffic.
PERFORMANCE, DISTRIBUTION, & AVAILABILITY
DDoS scrubbing services are a bit different from CDN-based services for a few reasons.

First, most DDoS services are on-demand, so the majority of their capacity is likely available and not already consumed by legitimate traffic.

They also tend to have a different architecture than CDNs, with a smaller number of higher capacity data centers, typically called scrubbing centers.

Any DDoS scrubbing service with high capacity but a limited or regional footprint will have a performance impact as traffic could have to be routed over multiple hops.

Additionally, depending on where your users are located in relation to the scrubbing centers on the front end and where your data centers are located on the back-end, there will be a range of increased application latency with a DDoS scrubbing service. For a cloud-based network security solution, this may not be an issue. Nevertheless, latency is a consideration for choosing CDN-based protection vs. a DDoS scrubbing service.

In the example shown in Figure 3, the service has two scrubbing centers in the U.S., which should be adequate for U.S. coverage, but there is only one scrubbing center in the Asia-Pacific region.

That means, whenever you turn on the service, users in China, for example, must route through Singapore to get to an application in Japan. This is not ideal, and the latency issues inherent with this type of architecture will be exacerbated.

**WHILE PERFORMANCE IS IMPORTANT, AVAILABILITY IS CRUCIAL**

One thing we know: All technology fails at some point. If one scrubbing center goes down, users will have to route through an alternate scrubbing center. In our example, with only one scrubbing center in-region, users in Italy would have to route through the east coast of the U.S. to get to an application in London. This clearly is not an ideal situation, and users are going to be affected.

As you can see, not all clouds are created equal, and a single type of cloud may not be able to supply all of your network security or performance needs.
HOW AKAMAI SOLVES THESE PROBLEMS
Akamai offers fully integrated solutions incorporating both CDN-based mitigation and a DDoS scrubbing service in a global network of servers supported by data-driven algorithms and automation, along with expert industry networking and security specialists. Depending on what your requirements are, you can choose one or the other, or both.

THE WORLD’S LARGEST CDN WITH INTERNET SCALE
Akamai has deployed the most pervasive, highly-distributed CDN with more than 216,000 servers in more than 120 countries and within more than 1,500 networks around the world. Because of this reach, we get closer to end users, closer to your applications, and closer to attackers than anyone else.

We have delivered 41 Tbps of record web traffic on our CDN platform. At any given time, we are delivering an average of between 20-24 Tbps of traffic. That means we typically have between 10-15 Tbps of available capacity to absorb attacks. Now that is scale – and that is why having enough available capacity to mitigate the largest DDoS attacks is not something Akamai clients need to worry about.

SEVEN GLOBAL SCRUBBING CENTERS TO PROTECT AGAINST DDoS ATTACKS
Akamai’s DDoS scrubbing service is built on a separate network of seven global scrubbing centers in San Jose, CA, Ashburn, VA, London, Frankfurt, Hong Kong, Sydney, and Tokyo. This delivers a robust, highly available global footprint for protecting your data center from DDoS attacks.

We have 3.2 Tbps of available network capacity on this network to support on-demand and always-on traffic around the world, with in-region redundancy. This is the largest network available for a DDoS scrubbing service.

MORE THAN ENOUGH SCALE, EITHER WAY
With Akamai, regardless of whether you choose our CDN-based or our DDoS scrubbing solution, there is enough available capacity to mitigate the largest DDoS attacks.

A CLOUD PLATFORM WITH INTERNET SCALE

More than 216,000 servers in over 120 countries and within more than 1,500 networks around the world.
THE BENEFITS OF COLLECTIVE INTELLIGENCE
As a cloud security vendor gains experience and expertise from preventing and mitigating DDoS and web attacks, its accumulated expertise benefits its entire customer base if, when, and before they are attacked.

FOR EXAMPLE, a Kona Site Defender customer notified us they were under attack and asked us to investigate. We found an attacker had hammered their site with more than 2,000 unique Remote File Inclusion (RFI) exploit attempts. Regardless of the number of attempts, the more important issue was that this was the first time Akamai had seen somebody looking for this vulnerability.

Based on our experience, we dove deeper. We suspected Google’s™ recent update of skipfish, an open source, fully automated, active web application security reconnaissance tool that scans for RFI exploits. We were right. This attacker had likely downloaded the tool and pointed it at our customer.

We decided to investigate whether other customers had been targeted as well.

BRINGING IN THE BIG DATA
Using our Cloud Security Intelligence (CSI) big-data analysis engine, we identified that this attacker had targeted 34 sites with more than 24,000 individual exploit attempts. That was alarming, so we investigated whether other attackers might be launching the same attacks. It turned out this one attacker was part of a 272-strong botnet. The botnet had launched attacks against almost 1,700 different applications on the Akamai Intelligent Platform™ – targeting hundreds of Akamai customers – with more than 1.3 million exploit attempts in two weeks.

Yet only one customer realized that they were under attack and called Akamai.

All of the other customers – and many were not even network security customers – were unaware someone was targeting their sites. However, all of our customers benefitted from the collective intelligence that Akamai gathered from an attack against a single customer.

How? We immediately notified all of our customers of the attacks, issued a threat advisory with a custom rule to potentially impacted customers, and updated our proprietary Kona Rule Set to protect all customers against these types of attacks.

"Bot management is a never-ending game of cat and mouse. Vendors need visibility into Global web traffic so they can stay ahead in the game."

THE BENEFITS OF COLLECTIVE INTELLIGENCE

HOW AKAMAI APPLIES COLLECTIVE INTELLIGENCE

Collective intelligence is not an inherent benefit of the cloud. While many vendors claim to provide collective intelligence, without significant scale, clients, and traffic volume there will be limited value.

We leverage the scale of the Akamai Intelligent Platform™, our huge traffic volume, the thousands of customers of every size we support, and our proprietary Kona Rule Set to better protect every client from incidents discovered at any single customer. Visibility into global web traffic reveals how it is evolving, including the development and mutation of bot traffic.

IP REPUTATION

Another form of collective intelligence is IP reputation. This practice assigns a reputation score for IP addresses based on past behavior, such as being involved in DDoS attacks, web attacks, or scanning and scraping activity. Armed with this information, organizations can choose whether to proactively block potentially malicious IP addresses from accessing their websites and applications.

However, most IP reputation products use limited or third-party data sources that can be out of date or have varying degrees of quality. This means that you could be left blocking legitimate users while allowing access to malicious IPs, putting your site and applications at risk.

As a practical matter, it often means that you are left with a binary risk score – is it an attacker or not? Is it a scraper or not? Has the IP reputation product seen that IP address performing any malicious activity, regardless of how often, how severe, or how long ago?

This can have major implications, as IP addresses often change hands, leaving a new user with a bad reputation, and different companies have different perceptions of risk.

Effective IP reputation scoring requires a huge volume of internally collected data, thousands of clients of all sizes, and the ability to quickly analyze and take action. With this information, you can provide additional information about each IP address, such as how much malicious activity was observed, how long ago it occurred, and an assessment of the risk that it entails.

This allows you to increase and decrease the risk score of that IP address based on recent activity, giving you the latest and most accurate assessment of risk. This helps you make a better decision as to whether or not to grant access to your website.

Akamai’s unprecedented view of web traffic gives us access to more web client data than any other network security provider. We use advanced heuristics and algorithms to create a reputation score for every IP address that crosses our platform. With our IP reputation solution, we give you a risk score from 1 to 10 in each category, based on recently observed activities, so you can take the right action for your specific business and risk-management needs.

FAST FACTS:
Akamai’s Cloud Security Intelligence (CSI)

• CSI ingests up to 20 Terabytes of new attack data each day with continuous analysis of 2 Petabytes of data at any given point in time

• CSI data is used to identify and track over 1,300 known bots in 15 categories of legitimate services and to refine real-time bot detection rules

• Data pulled from up to 80 million WAF rule triggers per hour – and 600,000 log lines per second – updates and improves the Kona Rule Set

• A dedicated threat research team runs 8,000 queries per day, leveraging the power of CSI. Analysis and insights gained from CSI are featured in the quarterly release of the State of the Internet Security Report.
AN IP REPUTATION CASE STUDY

A U.S.-based national retailer had Akamai’s WAF deployed without our IP reputation service. When we examined their WAF rule triggers for a 24-hour period, we found it had detected and blocked malicious requests from 259 IP addresses. That is indicative of the effectiveness of a WAF solution in protecting a single customer.

However, when we went back and looked up all the IP addresses that had accessed this customer’s site with our IP reputation database (Client Reputation), we saw an additional 1,549 IP addresses that were known to have performed malicious activity against other Akamai customers.

This illustrates the power of collective intelligence and Akamai’s visibility into attacks against other customers.

FIGURE 5: Using Akamai’s IP reputation database, an additional 1,549 IPs were identified as malicious.
UNDERSTANDING WAF ACCURACY
When it comes to understanding WAF accuracy, there are usually more questions than straight answers.

• What does accuracy really mean?

• Why do some vendors claim less than 1% false positives?

Comparing accuracy claims from different vendors is tricky. Comparing Vendor A’s accuracy and Vendor B’s accuracy is meaningless unless both numbers were measured with the same test.

**HERE IS WHY:** Let us say Vendor A tests against 10 attack vectors. They run their test, catch them all, and can claim 100% accuracy.

Now let us say Vendor B tests against 100 attack vectors – 10 times as many as Vendor A. They run a test, catch the same 10 vectors as Vendor B, plus another 80 vectors, but they miss the last 10. As a result, they receive an accuracy score of only 90%. This is why you have to understand what’s being tested for and why it is so difficult to compare one vendor’s accuracy number to another.

Many times, a vendor will tout a high accuracy rating from a third-party test. However, if you do a little research, you might find that every vendor tested measured 99.5% or better. That does not say much about the quality or the usefulness of the test. More importantly, you need to understand the breadth of the test.

“Advanced threat actors are leveraging automated attacks and logic-based exploits, which require modern WAF solutions to properly address.”

WHAT YOU NEED TO KNOW ABOUT FALSE POSITIVES

A false positive is a legitimate request that a network security solution has falsely identified as an attack. In other words, it means a legitimate user has been stopped.

Some vendors like to tout that they have <.01% false positives, however that can be misleading and represents only part of the picture.

Many WAF vendors like to tune for low false positives, but it can come at the expense of high false negatives. This is dangerous, because a false negative is an attack that the solution did not catch and allowed the malicious actor access to the application.

Consequently, a vendor that claims low false positives, but says nothing about false negatives, should be a real concern.

A ZERO FALSE POSITIVE EXAMPLE

Security pros know that it is easy for any security solution to have 0% false positives. All they have to do is turn off all network security controls and allow all traffic through. Now you will have no false positives and never accidentally block legitimate users, because you are not blocking anything.

Conversely, it is also easy for any security solution to have 0% false negatives: block everything, including legitimate users.

Of course, neither approach leads to effective security. That is why you need to talk to vendors about false positives and false negatives alike.

"For a real comparison, you need vendors to show you how these features make WAF policies easier and better in practice. If these capabilities help tune your WAF policies without a lot of work on your part, you’re getting huge value. If it’s just another way to look at data, it’s not worth it."

– Securosis, Maximizing WAF Value, Apr. 29, 2016.
CONTINUOUS IMPROVEMENT

At Akamai, we talk about both false positives and false negatives.

We test our WAF with an automated testing framework on a daily basis. We subject it to more than 12,000 unique legitimate HTTP requests that we have culled from customer traffic, along with more than 700 different attack vectors. We analyze the full HTTP response and continuously fine-tune our rules to drive out false positives and false negatives.

It is very easy to create a high-scoring accuracy number, but that is not our goal. We make it more difficult on ourselves because we aim to continuously improve our WAF. That is reflected in the data we use to test it, including traffic to customer applications that we know are prone to high false positives.

Kona Site Defender
WAF Foundation Methodology:

1. **Scale**: More than 216,000 servers in place and always on, around the world.

2. **Reverse Proxy**: Kona automatically drops traffic from non-standard ports.

3. **Geo-based Blocking**: Customer-selected request refusal by location.

4. **Validation**: Kona checks against known list of attackers: employs a positive or negative security model (black hat/white hat lists).

5. **Throttle Control**: Automatically blocks requests that are too fast or too slow (anomaly scoring).

6. **Continuous Updates**: Akamai’s Kona Rule WAF Set is continually updated and refined, based on deep visibility into the web.

7. **Performance**: Caching, both dynamic and static, to speedily serve requests.

"Akamai is a powerhouse in the WAF market. Kona Site Defender provides reliable detection rates without wasting customers’ time & resources on false positives."


FIGURE 6: It is important to go beyond false negatives and false positives when considering a WAF.
STOPPING ATTACKS FAST
UNDERSTANDING TIME-TO-MITIGATE
Any vendor can say they mitigate attacks fast. However, when you are planning for the security of your business, you want to know how fast they will respond when you are actually under attack.

One key metric is to ask for their Service Level Agreement (SLA) – and not just any SLA, but an SLA specific to the speed and quality of mitigation.

DISSECTING VENDOR RESPONSE CLAIMS
Here is a very typical statement that was pulled from the website of a cloud-based DDoS protection service, “Industry-leading SLAs for uptime and response times to DDoS attacks within minutes.”

ON THE SURFACE, THIS LOOKS GOOD.
But this is not actually talking about mitigation. It is talking about uptime. Now, you certainly need an uptime SLA. However, the thing that you should demand from every cloud platform is a 100% uptime SLA, because you are putting it in front of your application, and you do not want a single point of failure.

RESPONSE TIMES
Let us look at the second part of that claim, “response times to DDoS attacks within minutes.”

We all want a fast response, but response times do not equate to mitigation. Responding to an attack is not the same as stopping one.

Akamai has performance solutions that come with response time SLAs. That means when you call, email, or log a ticket, we will get back to you within X amount of time.

If a vendor only offers response-time SLAs, all this says is that they will start looking at your attack quickly. It still does not explain how long it will take to mitigate the attack once they start looking at it.
WITHIN MINUTES SOUNDS FAST

Most mitigation relies on DDoS scrubbing solutions, which are frequently deployed in on-demand configurations. Most of the time, your traffic goes directly from end users to your applications. When you come under attack, you need to make a BGP route advertisement change to reroute traffic onto the DDoS scrubbing platform before the vendor can start to mitigate the attack.

That BGP route advertisement change will usually propagate across the Internet within minutes.

So saying that you can respond to DDoS attacks within minutes only means that a cloud provider can start investigating the attack once your traffic is routed onto its cloud platform.

It is critical to have specific and contractually guaranteed mitigation SLAs. This is a tangible, written-in-stone metric you can use to objectively compare vendors.

AKAMAI TIME-TO-MITIGATE SLA

Akamai stands behind our claims with a time-to-mitigate SLA.

Sure, we respond to attacks fast, just like everybody else. We have response-time SLAs, just like everybody else. However, from the moment your traffic is on our platform, we also have an SLA that says we will mitigate the attack within X number of minutes, depending on the attack vector used.

This is not a vague marketing claim; it is a commitment written into a legal contract and backed by legal remedies. It is a commitment that our Security Operations Center (SOC) team is willing to make because they know they will always beat it, handily. You should worry if a vendor is not willing to make that commitment.

AUTOMATIC MITIGATION

Many vendors will say their technology or solution automatically mitigates attacks. It is preloaded with signatures and responds to attacks within seconds.

Akamai has this too. So why are our SLAs in the minutes and not seconds? Because SLAs are about worst-case, not average, response. So when a vendor commits to an SLA, that means they believe they will meet it, even in a worst-case scenario.

The fact is, it is not about the tools, it is about the people and processes behind the tools. Your automated response may be great for stopping most attacks, but there is always an attack that gets around it and requires the SOC to investigate and adapt.

That is why, despite all of the claims of automatic mitigation within seconds, few will commit to a time-to-mitigate SLA.
SECURITY OPERATIONS CENTER (SOC)
COMPARING SOCs
The SOC has the people that are going to support you when you come under attack. That means the quality of service you receive will be directly related to the quality of the SOC. The security of your business will depend on it.

By asking the right questions, you can better compare different SOC organizations.

FOR EXAMPLE, let us assume there is a cloud-based DDoS protection service on the market today that claims to protect you with their 24/7 SOC. Great.

HOWEVER, when you start asking questions, you find out:

- They have five people in their SOC
- They have four overlapping shifts and one person on call in case of illness or emergencies

That means there is only one person on staff at any point in time to help hundreds of customers. It makes you wonder what kind of service you can expect when you and a second customer are attacked at the same time.

Akamai’s SOC is a global network of five facilities staffed with highly trained security experts that deal with network security issues on an organizational and technical level. A global presence enables us to better help our customers, wherever they are located.

We have more than 150 people in our SOC. This is independent of the people in our security professional services organization. Because we have more than 150 people in our SOC, we can staff in overlapping shifts, and there is always an hour overlap and a clean hand-off between shifts if they are responding to an attack on your behalf.

As with anything else, the more you do something, and the longer you do something, the better you get at it. The Akamai SOC mitigates more attacks than anyone else and has been doing it for longer than anyone else – more than 12 years. This assures an experience factor – learned from early attacks – that supports the mitigation of hundreds of individual attack events each week.

And of course, because of all that, our SOC can offer a time-to-mitigate SLA.

DIGGING INTO DIFFERENCES
WHY YOU NEED METRICS

FIGURE 7: A 24/7 SOC is not enough if there are only a few people working there
DEFENSE IN DEPTH
On-premise mitigation appliances and enterprise data centers quickly become overwhelmed by high-volume attacks. Once the traffic arrives at your door, you have to deal with all of it. And if you cannot, you have lost the battle before the appliance can filter it.

Due to the limitations of this type of equipment, you will hear vendors recommend a multi-layer defense, or defense in depth, which usually involves blocking attack traffic in the cloud, before it gets to you.

MULTI-LAYERED DEFENSE AND DEFENSE IN DEPTH
Multiple layers of defense are the concept of having your applications or infrastructure in the middle, with a ring of security protection around them.

It is possible the protections you have in place today are provided by on-premises hardware, and that is great. But when we consider how the threat landscape is changing, we start seeing the need for another layer of defense. Only the cloud offers the scale needed to respond to the largest attacks.

MATURE CLOUD VS. STARTUP CLOUD
Your on-premises vendor will often try to get you to deploy their cloud-based solution as well.

It seems to make perfect sense to deploy their cloud-based solution as the additional layer of defense, but the truth is not as clear-cut as it might seem.

THE ONE HUGE HOLE IN THIS LOGIC: DEFENSE IN DEPTH
The basic premise of defense in depth is that no network security solution is 100% effective. This is true for any technology, because every solution will have different strengths and weaknesses.

By deploying multiple layers of defense built on the same underlying technology or hardware, you put yourself at risk. You don’t actually get defense in depth because all of those layers are going to have:

- The same weaknesses
- The same gaps
- The same holes for attackers to exploit to get at your applications

THE SOLUTION TO THIS PROBLEM
The best approach is to layer multiple, best-of-breed technologies on top of each other. This approach delivers multiple layers of defense that have different strengths and weaknesses, making it harder for an attacker to get all of the way through to your applications.

THAT’S TRUE DEFENSE IN DEPTH.
True multi-layered security – which is the industry-accepted approach – means a serious consideration of best-of-breed cloud-based technology, like Akamai. Our security cloud can complement existing on-premises solutions you may already have today.

WITH BEST-OF-BREED DEFENSE IN DEPTH

FIGURE 8: A multi-layered approach to cloud security ensures a more comprehensive defense
RECAP

This e-book was created by Akamai to help address questions and misunderstandings related to cloud security.

**WE HOPE WE’VE ACHIEVED THIS GOAL.**
Here’s a summary of what we’ve covered in this e-book:

- **WHY CLOUD-BASED SECURITY MATTERS:** Scale and how today’s threat landscape is driving scale requirements
- **WHY SCALE MATTERS TODAY MORE THAN EVER:** Every vendor says they can stop the largest DDoS attacks, and you just have to trust them? How to understand the true picture
- **UNDERSTANDING VENDOR CAPACITIES:** Every DDoS protection service operates in a global infrastructure with multiple data centers. But do their capacity claims hold up?
- **DDoS SCRUBBING VS. CDN-BASED SECURITY SERVICES:** Which solution or solutions make sense for your organization’s needs?
- **COLLECTIVE INTELLIGENCE:** Intelligence from the power of many clients of all sizes, many networks, and mega traffic
- **IP REPUTATION:** Taking collective intelligence one step further
- **UNDERSTANDING WAF ACCURACY NUMBERS:** Why comparing accuracy claims may be completely meaningless
- **UNDERSTANDING TIME-TO-MITIGATE CLAIMS:** Akamai contractually provides SLAs specific to speed and quality of mitigation
- **COMPARING SOCs:** If every vendor claims to have a 24/7 SOC, what’s the difference?
- **MULTI-LAYERED DEFENSE:** Will a single vendor solution provide defense in depth or simply leave you with a common weakness?

To learn more about improving cloud security for your brand, visit [WWW.AKAMAI.COM/CLOUD-SECURITY](http://WWW.AKAMAI.COM/CLOUD-SECURITY)

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company’s advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit [www.akamai.com](http://www.akamai.com) or [blogs.akamai.com](http://blogs.akamai.com), and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on [www.akamai.com/locations](http://www.akamai.com/locations).

©2016 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 12/16.