FS-ISAC

From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector

June 2025

Contents

Executive Summary

The financial services sector is a prime target for distributed denial-of-service (DDoS) attacks. These attacks disrupt interactions between customers and their financial services providers by slowing or shutting down customer-facing websites and applications. Some attacks disrupt interactions between financial firms and third-party service providers, and even their employees, by preventing access and communication. While the motivations for DDoS attacks vary, the risks of operational downtime and reputational harm can impact their targets and cause an erosion of trust in the security of the company.

Today's DDoS attacks aren't just simple traffic floods. Sophisticated threat actors are launching precision-targeted, multi-dimensional assault strategies that exploit complex vulnerabilities in financial services' cybersecurity.

To help executives prepare for this new level of threat, this report provides:

- Analysis of the current DDoS threat landscape, including dominant attack types and threat actors
- Our new DDoS Maturity Model — a structured framework to help firms evaluate their capabilities and map them to current DDoS threats
- Fundamental cyber practices for managing DDoS threats, applicable to firms at all levels of maturity, and a guide to selecting DDoS mitigation providers

DDoS attacks will remain a favored tactic due to their low barrier to entry, high impact, and built-in anonymity. The sector's expanding attack surface offers attackers more opportunities — and today's DDoS attacks are smarter, more persistent, and better tailored to victims' business models than in past years.

As the threat landscape evolves and the risks to financial services operations, profitability, and reputations increase, the sector must recognize that DDoS attacks are much more than a nuisance — they're a strategic threat.

The data in this report is sourced from Akamai and FS-ISAC members.

See the trajectory of DDoS attack trends with the 2023 and 2024 FS-ISAC/Akamai reports.

The Evolution of DDoS: Return of the Hacktivists

Read here ↗

DDoS: Here to Stay

Read here ↗

FS-ISAC members will also have access to upcoming technical guidance on increasing DDoS maturity.

DDoS Trends: Volumetric and Application Layer Attacks

The financial services sector is at increasing risk from two types of attack across firms' technology stack: volumetric and application layer. See Appendix A for more information on these attacks.

Volumetric Attacks on the Rise

The financial services sector was the world's top target in 2023 and 2024 for volumetric DDoS attacks.

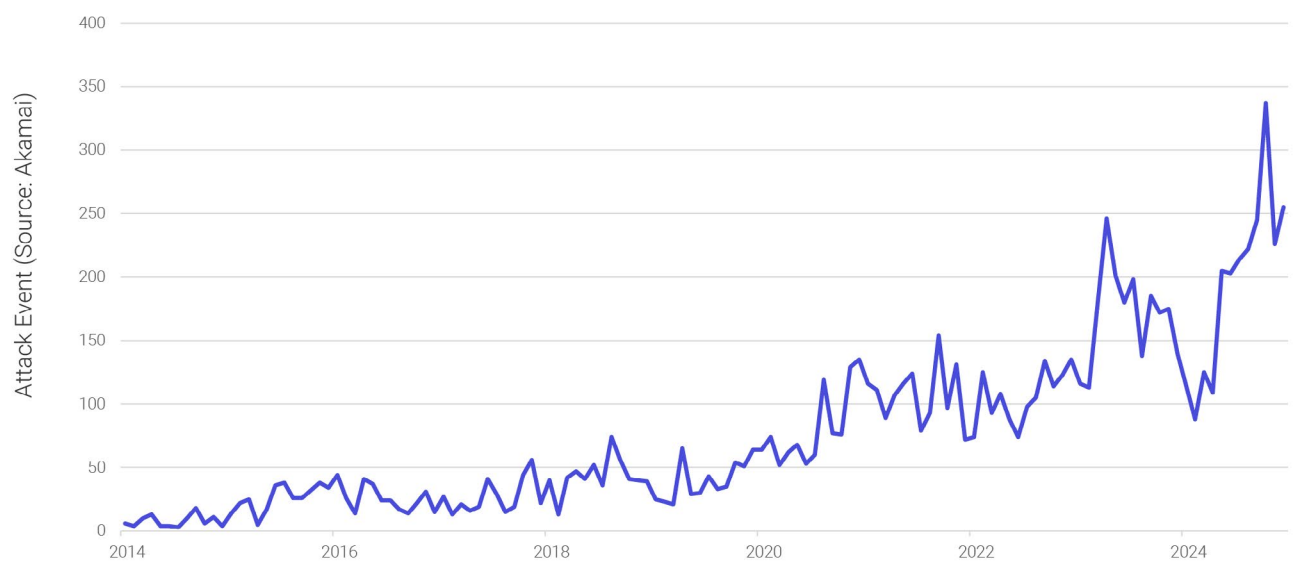
Campaigns range from opportunistic traffic floods to precise and very sophisticated attacks, and the motivation is not always known.

Akamai's volumetric DDoS attack data shows tracking of each attack against a company as an event. Each event can include hundreds, millions, or billions of individual malicious requests. Those requests are combined into a single volumetric attack event. As the graph, volumetric attacks on the financial services sector have been increasing for several years.

Volumetric DDoS Attacks

Volumetric attacks send enormous volumes of traffic — hence, the term volumetric — to overwhelm the capacity of the targeted server or network and cause it to slow down or fail.

Volumetric Attacks on Financial Services, 2014-2024



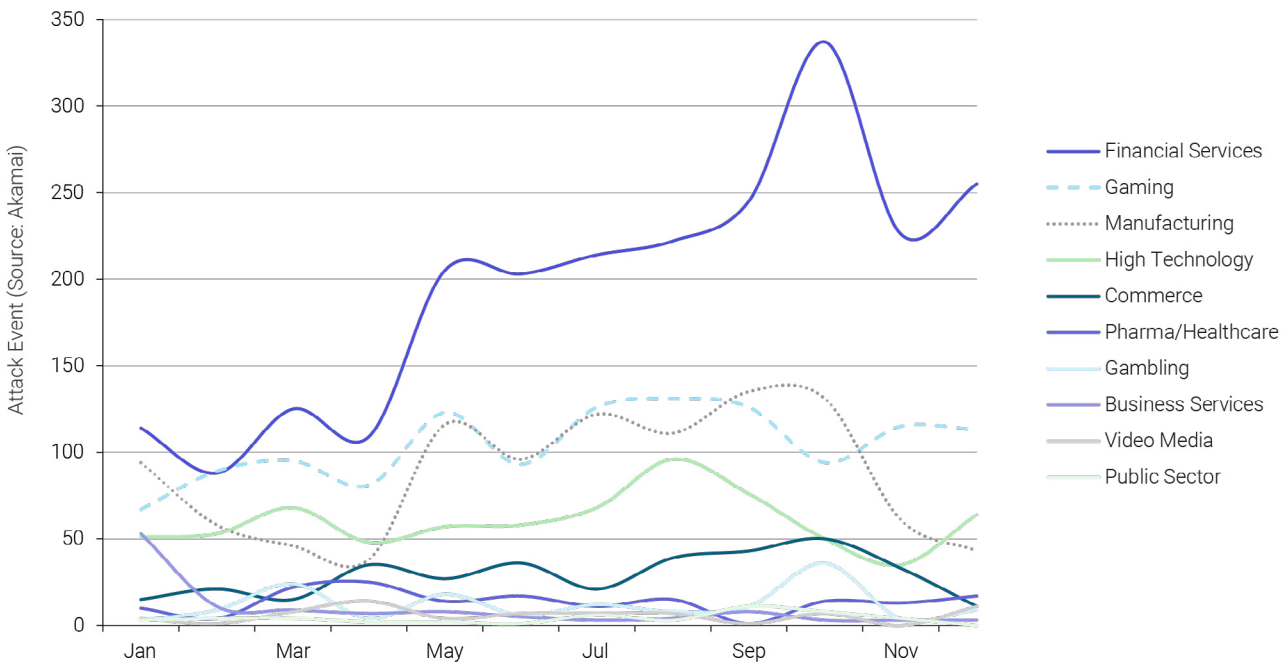
The financial sector experienced a major spike in volumetric attacks in October 2024, according to Akamai's data. FS-ISAC members began reporting more DDoS attacks at the same time. Many of the reported attacks shared overlapping attack vectors, suggesting that the threat actors are (a) the same, (b) collaborating, and/or (c) relying on common infrastructure or DDoS-as-a-Service providers. Overall, FS-ISAC members reported limited impact in most cases.

The frequency of DDoS events does not always reflect their severity and attack intensity – substantial spikes were recorded during periods of otherwise minimal DDoS activity. This highlights the importance of evaluating both the number of incidents and the scale of traffic to fully understand the impact and risk of DDoS attacks.

Overall, technological advancements have dramatically increased the power and capabilities of DDoS attackers. Today's bandwidth and computational resources enable the launch of adaptable, powerful, and cost-effective DDoS attacks. Many threat actors deploy virtual machine (VM) botnets to conduct attacks more efficiently by harnessing computational resources across numerous VMs and Internet of Things (IoT) devices. This approach exploits the distributed nature of cloud services, making attacks more difficult to mitigate and trace.

It is important to note that while an overall increase of volumetric DDoS attacks is observed, the financial services sector is experiencing a disproportionately large increase compared to other industries, according to Akamai's data. Though many of these attacks were related to the US elections and the escalation of conflict in the Middle East, hacktivist groups claimed responsibility for a limited number of attacks in 2024. The broader cluster of incidents remains unattributed, and the motivations of the threat actors are still unclear.

Volumetric Attack Trends by Sector in 2024



Application Layer: The Growing Threat to APIs and Web Applications

Application layer DDoS attacks against the financial sector increased 23% between 2023 and 2024 (see Appendix A for more information on application layer attacks).

Application attacks can target different aspects of an application's infrastructure at Layer 7, either web applications or Application Programming Interfaces (APIs).

- Web application attacks target user-facing components of web applications, such as login pages.
- Attacks on APIs target application logic – such as login forms, payment gateways, or endpoints – and often require fewer resources to cause significant service degradation.

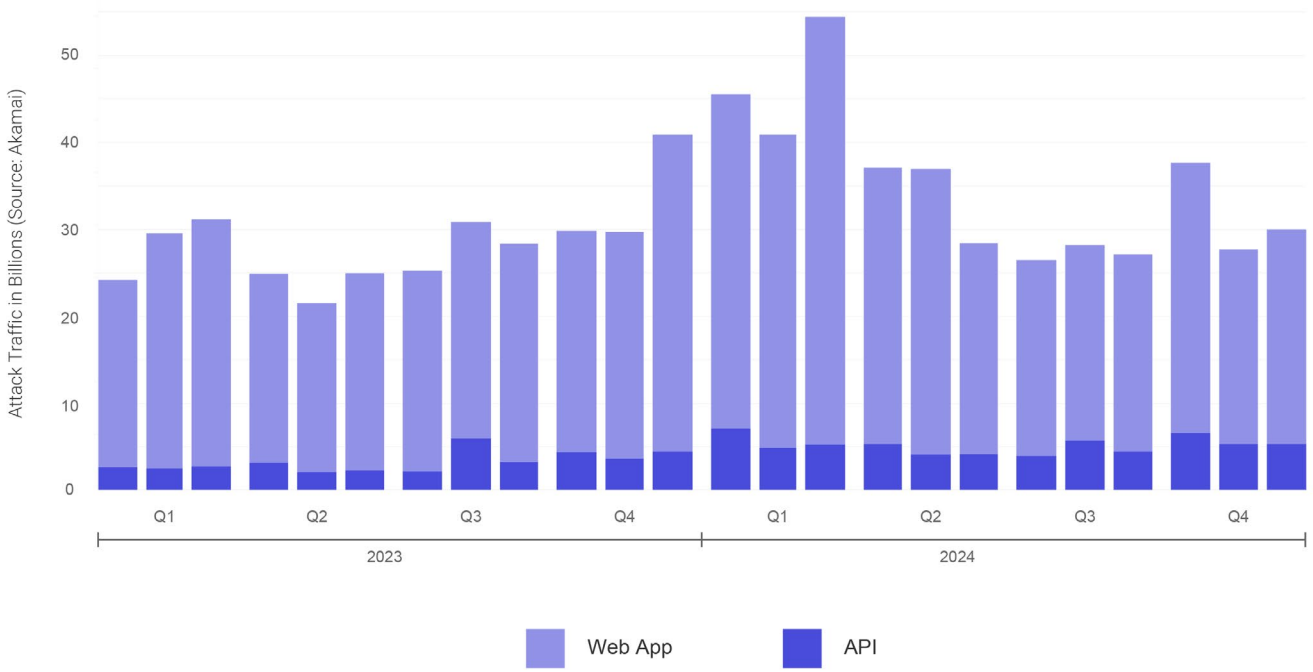
Web application attacks are comparatively simple exploits that typically target the parts of an application visible to consumers. Akamai data shows a 19% increase in DDoS attacks launched against web applications in the financial services sector between 2023 and 2024.

API attacks require a deeper understanding of the target's structure and behavior – such as which APIs are exposed, which are vulnerable, and which are business-critical. Akamai found a substantial increase – 58% – of application layer DDoS attacks targeting APIs in the financial services sector between 2023 and 2024.

The sector's increasing reliance on web applications and APIs expand its attack surface and the potential for DDoS attacks. The sector is likely to remain an appealing target due to its critical role in global economic infrastructure, the high value of financial data, and the potential for significant disruption.

While volumetric attacks are more numerous, application layer attacks are disproportionately impactful. Their profile is stealthier than that of volumetric attacks and they tend to bypass traditional defenses more successfully, which makes application layer DDoS attacks a priority risk despite lower raw volume.

Financial Sector Application Layer DDoS Attack Traffic, 2023-2024



This graph shows Akamai's tracking of application layer attack traffic by volume to compare the amount of malicious traffic targeting web vs API endpoints.

Increasing Sophistication of DDoS Attacks

As the number of volumetric DDoS attacks increased, so did the sophistication of the attacks – particularly since the last quarter of 2024. Indeed, the most effective DDoS campaigns in 2024 were characterized by strategic reconnaissance and agile execution rather than simple volume.

In 2024, threat actors increasingly employed advanced multi-vector DDoS strategies that incorporated systematic probing and adaptive tactics. This demonstrates an ability to analyze defenses in real time and dynamically adjust methods to evade automated protections. This marks a clear evolution in attacker capability, resources, and intent, and increases the threat of DDoS attacks against the financial services sector.

In general, Akamai and FS-ISAC members observed the following adversarial patterns and characteristics in 2024:

- **Highly systematic and methodical approaches aimed at circumventing DDoS defense mechanisms.** Threat actors tested a wide range of attack vectors, often at low traffic volumes, to assess the effectiveness of different techniques. While this tactic is not new, it was applied skillfully and in parallel across numerous financial institutions over extended periods.

- **Initial probing phase to gain intelligence, later used to deploy multi-vector DDoS attacks with significant traffic volumes.** Notably, the traffic volume of these attacks was high, but moderate compared to historically large-scale DDoS events and remained below the advertised capacity limits of most DDoS mitigation solutions. These attacks frequently targeted multiple financial organizations in parallel and were sustained over several weeks to months, suggesting the attackers possessed substantial resources.

- **Bypassing automated DDoS defenses and disabling typical on-premise network (proxy, firewall, load-balancer) infrastructure.** Despite the moderate traffic volumes, these attacks proved effective in causing service disruptions. In several cases, service outages persisted for days, resulting in a notable impact on end users.

Overall, the nature of these attacks suggests skilled, well-organized, motivated threat actors willing to invest time and effort to study their target's infrastructure.

Geopolitical Influence

The geopolitical landscape continues to play a major role in shaping the priorities and behaviors of cybercriminals. Ongoing conflicts — such as the Russia/Ukraine and Hamas/Israel wars as well as increasing tensions in the Middle East — have altered the DDoS cyber threat landscape significantly.

While some DDoS attacks are launched by state-sponsored actors, geopolitical developments also inspire hacktivists. A notable example occurred in October 2024, when a DDoS campaign targeted multiple Australian financial institutions. While an attack on one major Australian bank was claimed by the pro-Palestinian hacktivist group RipperSec, the majority of the other attacks went unclaimed. The timing coincided with a series of significant geopolitical events, including:

- The meeting of NATO Defense Ministers in Brussels, attended for the first time by officials from Australia, Japan, New Zealand, and South Korea.
- Australia's announcement of military aid to Ukraine.
- An address to the European Council by Ukrainian President Volodymyr Zelensky.
- NATO's annual nuclear deterrence exercise, "Steadfast Noon," held in Europe.
- The targeted killing of Hamas leader Yahya Sinwar by Israeli forces in Rafah.

Hacktivism

Hacktivism is the use of cyber attacks as a form of digital protest or political expression. Some hacktivists belong to criminal groups furthering state-sponsored agendas.

Why Attribution Matters

Lack of attribution creates a significant intelligence gap. Until a threat actor is known, threat intelligence analysts may have difficulty identifying the underlying objectives and potential risks, making mitigation more challenging.

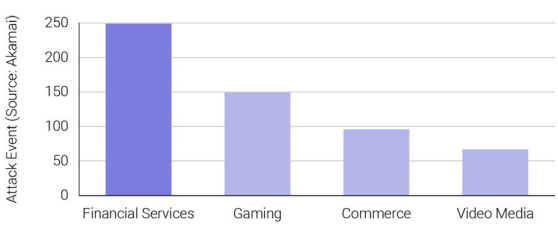
These overlapping events suggest a potential link between geopolitical tensions and DDoS attacks. However, because most attacks remain unattributed to an individual, geography, organization, or state sponsor, it is more difficult for threat intelligence analysts to map known methodologies and identify indicators of compromise, which are crucial components of developing actionable intelligence. The challenges of attributing some DDoS attacks relate to the use of DDoS-for-hire services – which are increasingly common – as well as sophisticated threat actors' use of DDoS as part of a broader offensive toolkit.

Regional Overview

APAC

The financial sector became the most targeted sector in the region, accounting for 38% of volumetric DDoS attacks, a sharp increase from 11% in 2023.

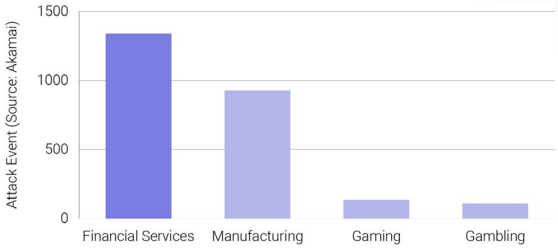
Volumetric Attacks in APAC, 2024



EMEA

Volumetric attack rates dropped to 49%, down from 66% in 2023, the peak of the geopolitically-motivated hacktivist attacks. Financial services remain a primary target.

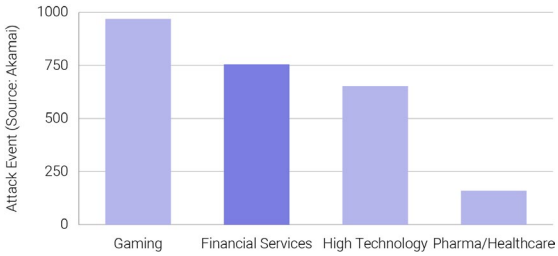
Volumetric Attacks in EMEA, 2024



NAM

The region's number of volumetric DDoS attacks is essentially unchanged at 27% in 2024 from 28% in 2023.

Volumetric Attacks in NAM, 2024



Notable DDoS Attacks in 2024

Jul

A major financial services company in Israel was attacked on 15 July via a globally distributed botnet.

The 30 July attack on Microsoft's Azure services caused a nearly 10-hour outage, took Office and Outlook offline, and impacted the financial sector.

Aug

On 27 August, a large institution headquartered in the US experienced the most significant DDoS attack observed in the past four years and the third-largest volumetric DDoS attack ever recorded on the Akamai Prolexic platform (which inspects traffic and applies mitigation controls). Despite the attack's intensity and duration, there was no impact on the institution or its legitimate users.

Oct

A record-breaking 29 October attack — part of a bigger campaign of hyper-volumetric DDoS attacks — was launched by a botnet on an internet service provider in Eastern Asia.

APAC experienced an unprecedented wave of DDoS attacks targeting over 20 unique financial institutions in six countries, according to Akamai research. These well-orchestrated DDoS attacks were likely launched by the same threat actor or hacker group.

Notable DDoS Threat Actors

BlackMeta

AKA DarkMeta, a pro-Palestinian hacktivist group that launched a sustained six-day application layer DDoS attack against a financial institution in the United Arab Emirates (UAE) in August 2024. This attack, notable for both its duration and intensity, was carried out using InfraShutdown, a DDoS-for-Hire service, underscoring the growing accessibility of such tools to ideologically motivated threat actors. Active since November 2023, BlackMeta has previously targeted organizations in Israel, the UAE, and the United States. BlackMeta's campaign was part of a broader protest of perceived injustices against Palestinians and Muslims. Their tactics echoed those used by other hacktivist groups, such as Anonymous Sudan, illustrating the evolving playbook of ideologically driven cyber operations.

NoName057(16)

One of the most persistent and active hacktivist groups that emerged in response to Russia's invasion of Ukraine, NoName057(16) developed the DDoSia tool, which attacks different targets daily, mainly in Europe. The governmental sector was its primary target in 2024; the financial sector was in the top five. The group's manifesto indicates a preference for targeting companies and organizations that express support for Ukraine or hold an "anti-Russia" stance. However, instances of collaboration with pro-Palestinian hacktivist groups have also been observed, highlighting the increasingly fluid alliances within the hacktivist landscape.

RipperSec

A pro-Palestinian hacktivist group likely based in Malaysia, RipperSec is reported to have claimed responsibility for DDoS attacks on a major Australian bank in October 2024. RipperSec is known for its focus on financial targets and advanced technical operations, often using a community-driven approach leveraging an estimated 2,000 members and forming alliances with other global hacker groups.

GorillaBot

A botnet that caused significant downtime in a number of financial institutions during the second half of 2024. Access to the platform is provided by a cryptocurrency-based subscription model and incorporates an unknown number of infected devices. In September 2024 the botnet issued over 300,000 attack commands with a daily peak of over 20,000 commands.

Unattributed Botnet

This botnet is likely responsible for a global DDoS campaign targeting the financial sector, specifically e-banking services, business-to-business application interfaces, services operating on non-standard ports, and dedicated internet access circuits used for secure, high-bandwidth connectivity. The campaign has been ongoing since October 2024 and uses a methodical approach to bypass DDoS defense controls, often employing probing attacks as reconnaissance to identify weak points or vulnerabilities. It is unclear whether the actors leveraging the botnet represent a single coordinated group, a collection of unrelated operators, or if the infrastructure is part of a DDoS-for-Hire service accessible to various actors with different motivations. FS-ISAC and its member institutions are actively investigating the botnet's origin and attribution.

Proactive Approaches to Mitigation

Solving for this DDoS threat landscape requires proactive detection, behavior-based analysis, and both automated and manual interventions — relying solely on automated response puts consistency and/or the quality of mitigation at risk. These controls must provide flexible operational and incident response and consistent testing capabilities.

Moreover, understanding attacker behavior — such as probing for API vulnerabilities, detecting unprotected infrastructure, or bypassing application-layer defenses — at the destination level enables more proactive and tailored countermeasures. Network traffic anomalies, such as unexpected surges, irregular request patterns, or activity from spoofed or untrusted sources, are often early indicators of DDoS campaigns and should be continuously baselined and monitored to inform rapid mitigation.

One often overlooked aspect of mitigation is a focus on upstream providers. Regularly reviewing third-party network and cloud dependencies for their own DDoS posture can prevent single points of failure and service degradation beyond an organization's direct control.

Other effective approaches include:

- Geo-IP filtering, which can cut exposure by blocking traffic from regions where the firm has no business operations.
- Dynamic traffic shaping to help manage attacks in real time, prioritizing critical services and shedding less important load when needed.
- Infrastructure diversity and defense in depth approaches, which reduce reliance on a single vendor and add resilience against provider-targeted attacks.
- Pre-agreed scrubbing support, which quickly triggers a response when thresholds or anomalies are detected.
- Positive security, or whitelisting, built into any implementation for network security and DDoS. This approach explicitly defines what is permitted and rejects everything else.
- Threat intelligence fed directly into edge defenses to help block known malicious traffic before it causes disruption.
- Regular DDoS playbook tests — whether through red team activity or tabletop exercises — to make sure plans work under pressure.

DDoS Maturity Model

A high level of cyber maturity reduces financial firms' risks, but cyber maturity differs among the sector's institutions. As the DDoS threat landscape becomes more diverse and sophisticated — and as institutions experience more attacks — firms can benefit by using the DDoS Maturity Model to assess their ability to withstand and respond to DDoS attacks.

This model is a structured approach that pinpoints where efficiency and maturity should increase substantially. This helps financial institutions increase resilience, prioritize investments, and facilitate ongoing improvement.

The framework for this methodology has five levels — from 1 to 5 — and can be tailored to the organization. Each level is described individually below. Please see Appendix B for the complete table.

Level 1: Initial		
Characteristics	Defensive Capabilities	Risks
> Business-side underestimates potential for DDoS attack and the threat to brand and revenue > Low level of cybersecurity maturity > No investment in DDoS defense > No threat intelligence or API/ endpoint inventory > Extreme vulnerability	> No Layer 3 and 4 or Web Application Firewall > No or ineffective mitigation measures > No baseline of "normal" traffic behavior > No logging or traffic visibility	> Easy target for attackers > Long service unavailability

Organizations that have never faced a significant DDoS attack often assume they are not attractive targets for threat actors — and as a result, they neglect to invest in DDoS mitigation. Such organizations are precisely the kind of enticing targets attackers seek.

Institutions at the initial stage of maturity typically lack basic Layer 3 and 4 or Web Application Firewall (WAF) protections. As a result, the impact of a DDoS attack can be prolonged — even those that are simple to mitigate — because defenders have little "know-how" and no effective mitigation measures. Institutions at this level often have no inventory of exposed APIs or endpoints and make no use of threat intelligence. This leaves them blind to potential threats and vulnerable to exploitation.

Level 2: Reactive		
Characteristics	Defensive Capabilities	Risks
> Fragmented security measures > No centralized strategy or coordination > Limited asset awareness > Few proof points from testing frameworks to evaluate their risk exposures	> Manual response during attacks > Manual blocking of malicious IPs > Minimal use of threat intelligence > Basic firewall rate caps > Some monitoring, but no anomaly detection	> Slow, ineffective, and easily overwhelmed mitigation > Service disruption until infrastructure rebuilt > Limited visibility into upstream infrastructure dependencies > Limited IP blocking due to firewall rate caps

Organizations at the early stages of DDoS maturity often rely on reactive defenses. Their security measures tend to be fragmented, lacking a centralized strategy, coordination, or sufficient testing framework proof points to evaluate their risk exposures. During an attack, they may attempt to block malicious IPs manually and are frequently limited by firewall rate caps, making mitigation slow, inefficient, and easy to overwhelm. While these companies typically have a basic awareness of their vulnerable assets and attack surface, this knowledge is often incomplete. Threat intelligence, if used at all, is applied only after an incident has occurred, limiting its value in preventing future attacks.

At this stage, infrastructure can be easily affected — even by unsophisticated attackers — with impact to service availability until the infrastructure can be rebuilt. It is essential for firms at this level of maturity to establish a formal DDoS risk management process, which enables them to systematically identify and assess threats and proactively implement mitigation strategies.

Level 3: Proactive		
Characteristics	Defensive Capabilities	Risks
> Risk-informed DDoS defense strategy > Formal policies and procedures > Current inventory of assets, APIs, and IP addresses > Regular vulnerability scans	> Volumetric and perimeter-based detection > WAF rulesets > Cloud-based DDoS mitigation services	> Slow detection of attack vectors > High potential for extended downtime from multi-layered attacks > Inconsistent protection across different protocol layers > Limited ability to respond to application-layer attacks

This proactive stage marks a critical shift toward a risk-informed DDoS defense strategy. Organizations at this level have formal policies and procedures, and maintain an up-to-date inventory of APIs, IP addresses, and host resources associated with those IP assignments (i.e., "IP day job"). They routinely scan for exposed endpoints to reduce their attack surface. Volumetric as well as perimeter-based DDoS detection mechanisms are in place, complemented by well-configured WAF rulesets. These approaches strengthen the firm's ability to detect and mitigate attacks before they escalate.

However, detecting attack vectors is slow at this stage, which results in extended downtime as the response is implemented. The layers may not have equal protections, so sophisticated attacks with multi-layer attack vectors can cause prolonged service unavailability.

Level 4: Managed		
Characteristics	Defensive Capabilities	Risks
> Standardized, repeatable, and mature processes integrated into broader risk management > Real-time asset visibility	> Advanced behavioral analysis > Integrated scrubbing capabilities > DDoS mitigation embedded beyond the Security Operations Center to crisis management and exercises > Threat intelligence for business risk mapping > Threat vector identification within minutes	> May still have moderate delays in detection/mitigation > Incident response may depend on external providers

At this level, institutions have achieved a standardized and mature approach to DDoS risk management. They operate with established, repeatable processes and a comprehensive risk management program, enabling them to effectively detect, respond to, and recover from DDoS threats — resulting in a more secure and resilient organization. They maintain full visibility into exposed assets and service dependencies, allowing for informed risk assessments. Their defenses include integrated scrubbing capabilities and advanced behavioral analysis to detect and understand attack patterns in real time. DDoS mitigation is fully embedded beyond the Security Operations Center (SOC) to crisis management and exercises, and threat intelligence is actively leveraged to map technical indicators to business risk exposure — enabling faster, more informed decision-making.

At this stage, attack vectors are detected and mitigation measures are employed in a reasonable time to limit impact. More sophisticated, multi-layered attacks as well as attacks against specific APIs can be detected and mitigated too.

Level 5: Adaptive		
Characteristics	Defensive Capabilities	Risks
> Real-time, dynamic response capability > Integrated, automated threat intelligence > Peer collaboration via FS-ISAC > Minimal gaps	> Threat vector identification within seconds or minutes > Automated mitigation > Protected dynamic/scaled environments	> Constant adaptation required to stay ahead > High resource investment

This level of cybersecurity maturity represents a truly preemptive and adaptive defense posture. Security teams at this stage have fine-tuned their practices to allow for real-time, dynamic responses to an ever-evolving threat landscape — ensuring the organization remains resilient and ahead of emerging cyber risks. Institutions maintain real-time visibility and map their digital assets, including shadow APIs (i.e., APIs in use without a cybersecurity team's oversight), and scale environments dynamically. Monitoring and detection capabilities are tightly integrated with automated threat intelligence feeds, enabling rapid identification of threats and a highly responsive security ecosystem.

At this stage, attack vectors are identified quickly and can be mitigated without much downtime. To further their defense, organizations collaborate with peer industry groups, such as FS-ISAC, to share their experience with others in the sector and exchange best practices.

References and Resources

Appendix A: Difference between Volumetric & Application Layer DDoS Attacks

Volumetric DDoS attacks target the network and transport layers (Layer 3 and Layer 4) by flooding systems with high volumes of traffic. Their goal is to overwhelm bandwidth, network resources, and infrastructure, disrupting service for all legitimate users. These types of attacks are often mitigated by traditional firewalls, network protection tools, and cloud protections.

Application layer (Layer 7) attacks target the application itself. These attacks bypass traditional network defenses and directly exhaust application server resources. They focus on resource-intensive features like specific web pages, database queries, etc. This makes them harder to detect as they often resemble normal user behavior. They can be mitigated with application layer signature systems like WAFs or systems that inspect application payloads, measuring and mitigating requests-per-second floods.

Application layer attacks have become increasingly common, particularly in the financial sector, where disrupting user access to web applications or API services can have serious consequences. While application layers are typically mitigated by diverse network protection strategies, application layer attacks are a major threat due to their ability to disrupt applications directly and the greater risk of over-mitigating legitimate clients.

Appendix B: DDoS Maturity Model

Level	Characteristics	Defensive Capabilities	Risks
Initial	> Business-side underestimates potential for DDoS attack and the threat to brand and revenue > Low level of cybersecurity maturity > No investment in DDoS defense > No threat intelligence or API/ endpoint inventory > Extreme vulnerability	> No Layer 3 or 4 or Web Application Firewall > No or ineffective mitigation measures > No baseline of "normal" traffic behavior > No logging or traffic visibility	> Easy target for attackers > Long service unavailability
Reactive	> Fragmented security measures > No centralized strategy or coordination > Limited asset awareness > Few proof points from testing frameworks to evaluate their risk exposures	> Manual response during attacks > Manual blocking of malicious IPs > Minimal use of threat intelligence > Basic firewall rate caps > Some monitoring, but no anomaly detection	> Slow, ineffective, and easily overwhelmed mitigation > Service disruption until infrastructure rebuilt > Limited visibility into upstream infrastructure dependencies > Limited IP blocking due to firewall rate caps
Proactive	> Risk-informed DDoS defense strategy > Formal policies and procedures > Current inventory of assets, APIs, and IP addresses > Regular scanning for vulnerabilities	> Volumetric and perimeter-based detection > WAF rulesets > Cloud-based DDoS mitigation services	> Slow detection of attack vectors > High potential for extended downtime from multi-layered attacks > Inconsistent protection across different protocol layers > Limited ability to respond to application-layer attacks
Managed	> Standardized, repeatable, and mature processes integrated into broader risk management > Real-time asset visibility	> Advanced behavioral analysis > Integrated scrubbing capabilities > DDoS mitigation embedded beyond the Security Operations Center to crisis management and exercises > Threat intelligence or business risk mapping > Threat vector identification within minutes	> May still have moderate delays in detection/mitigation > Incident response may depend on external providers
Adaptive	> Real-time, dynamic response capability > Integrated, automated threat intelligence > Peer collaboration via FS-ISAC > Minimal gaps	> Threat vector identification within seconds or minutes > Automated mitigation > Protected dynamic/scaled environments	> Constant adaptation required to stay ahead > High resource investment

Appendix C: Fundamentals of Cyber Hygiene for DDoS

Because cybersecurity involves active adversaries rather than potential disruption, threat trends should be constantly assessed. No framework of best practices exists to prevent DDoS but leveraging FS-ISAC's 15 Cyber Fundamentals is an industry best practice. Here are the key fundamentals that apply to DDoS:

- Know your network, especially hardware, configurations, and baselines.
- Regularly update and patch software – DDoS attackers can take advantage of zero days.
- Use backup systems to duplicate data and system configurations.
- Develop an incident response plan specific to attack type. DDoS attacks have real-time impact, so it's necessary to have a plan/process to rapidly mitigate impacts.
- Use firewalls, configured closed by default, with active blocking. Application firewalls are critical to safe customer access.
- Train employees on their role in cybersecurity – DDoS can kick off a crisis management event, so document roles in a RACI (Responsible, Accountable, Consulted, and Informed) matrix.
- Keep a log of system activity, which is necessary for investigations and trend analysis.
- Use secure configuration management.
- Incorporate application security controls.
- Harden API controls with testing and validation.

Additionally, Akamai's best practices include these processes:

- Review current capabilities against recent record-setting attacks and new attack methods.
- Have plans for volumetric, application, and DNS environments.
- Review critical IP spaces and subnets annually (they can be hard to track in dynamic organizations).
- Conduct periodic validation tests that include activating vendor incident response plans.

Appendix D: DDoS Protection Services Criteria

Financial services firms often find it more efficient and effective to outsource incident response – DDoS is a prime example to specialized services teams. There are many different as-a-service DDoS protection solutions available. These services detect attacks at an early stage, absorb the large-scale traffic of a DDoS attack, and can offer the resources necessary for effective mitigation. When choosing a DDoS mitigation service, the following questions are good reference points.

- What is the time-to-mitigation and uptime guarantee in the service agreement?
- What other detection or mitigation guarantees (e.g. consistency or quality of mitigation) are offered?
- Are volumetric, application, and DNS environments covered?
- Are there on-premise, cloud scrub, cloud proxy, or cloud elasticities in the design?
- Does the service allow for automation, adjustable risk appetite settings, and updates to new threats quickly?
- Does the service meet any compliance requirements?
- Does the service have a strong reputation in the industry and provide insights into best practices and playbooks?
- What are the notification and audit rights stipulated in the agreement?
- Does the service facilitate testing and validation exercises or require additional services to be enabled?
- Can the service provider's application work coincide with the organization's network environment?
- Does the protection fit the organization's business model, such as cloud/multi-cloud/hybrid environment, protection of the application layer, and protection for nontraditional web applications?

