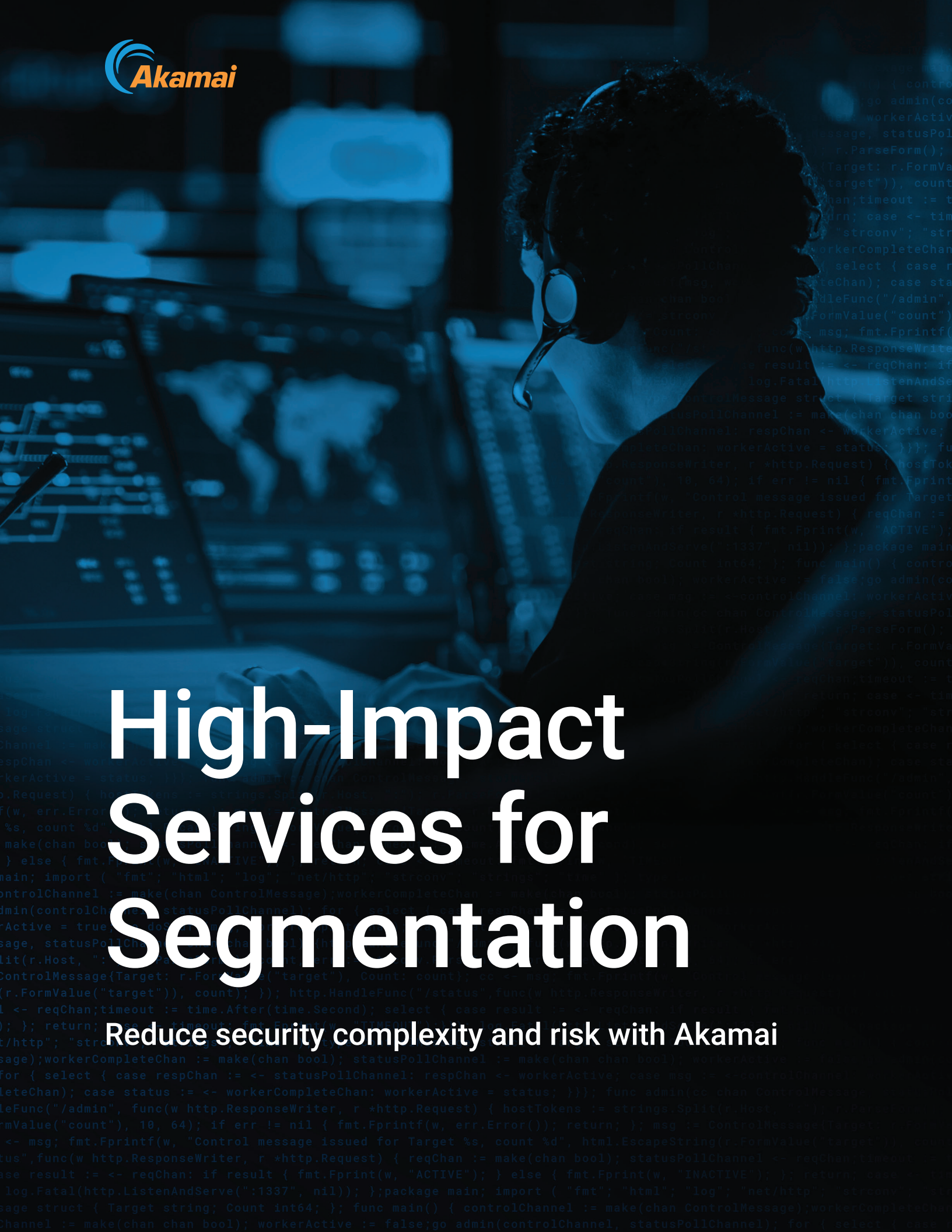

High-Impact Services for Segmentation

Reduce security complexity and risk with Akamai

Introduction

Protecting critical assets across on-premises data centers and public cloud environments is more important than ever. Increasingly, this requires specialized expertise to keep pace with new application deployment models in a rapidly evolving threat landscape. Our services experts are focused on turning your investment in our security portfolio into tangible, business-driven outcomes.

Akamai's microsegmentation services team is staffed by security experts with extensive training and real-world experience both in the private sector and in military intelligence organizations. Our flexible set of service offerings provides access to this specialized expertise as an extension of your in-house IT and security teams to implement best-in-class security from the data center to the cloud.

Customer journey

A typical customer journey starts with deployment and configuration via our Professional Services Delivery: We set up your environment, define assets and labels, and implement the policy for the first few use cases.

Then, we provide administrative and engineering training to some of the team members who are using the solution.

Additionally, Day-2 Operation Services may be used to continue and enhance the deployment (defining more assets and labels, as well as implementing policy for additional use cases), handle security incidents and improve the security posture, provide needed controls and reports for audits, and provide custom development to improve the integration with the customer's infrastructure.

Throughout the lifecycle of the solution, extensive support services will help resolve any issue that might occur, and our Customer Success team will ensure that you get the maximum value out of our product.

Customer journey with Akamai microsegmentation services

Customer success Ensuring that customers maximize the value of our product		
Professional Services Delivery Deployment of the product; implementation of first use cases	**Training** In-depth training and certification programs	**Day-2 Operation Services** Ongoing assets/labels/policy maintenance and expansions Security posture review and IR, audit prep, custom development and integration Technical Account Manager / Resident Engineer
Customer support services Technical support services: 24/7 support, designated engineer		

Professional Services Delivery

A comprehensive team consisting of security architects, project managers, and developers will work with your team to implement the Akamai Guardicore Segmentation platform. Depending on your needs, Akamai offers either a packaged set of deliverables, or a fixed-term implementation engineer. Regardless of the package you choose, our service offerings are tailored to ensure that your critical assets are protected.

Jumpstart

Jumpstart is designed for customers who need to accelerate their deployment of Akamai Guardicore Segmentation but prefer to implement and manage subsequent policies themselves with guidance from our experts. Whether you wish to segment your network environment, ringfence applications, or restrict access to servers, our engineers will design and implement your first policy objective, teaching you along the way and providing guidance as you implement subsequent policies on your own.

Our team will also work with you to plan the security architecture and understand any application design considerations. This includes defining and documenting the labeling strategy, labeling your assets in the platform, and formally creating and fine-tuning the policies to support your use case(s).

After Akamai completes your first policy implementation, our engineers will continue to provide your team with direct assistance with any future policy implementations, and will remain a part of your extended team until your deployment objectives are met.

Extended Jumpstart

For enterprises with multiple segmentation goals to achieve, Extended Jumpstart is ideal. Akamai experts will work with your teams to implement multiple segmentation policies, ramping up protection of your critical and crown jewel assets.

Our team will work with you to plan the security architecture and understand any application design considerations. This includes defining and documenting the labeling strategy, labeling your assets within the platform, and formally creating and fine-tuning the policies to support multiple security initiatives.

Typical policy objectives to implement

Whether you wish to segment your network environment, ringfence applications, or restrict access to servers, our engineers will work with you through every step of the journey to ensure your assets are protected.

As part of this offering, you can select multiple policy objectives or focus on a specific high-priority objective. Our engineers will implement the required labels and rules that form our policies until your assets are secured in alignment with your pre-identified objectives.

Some examples include:

- **Environment segmentation** — Servers from different environments will not be allowed to communicate, with the exception of explicitly allowed communications.
- **Application ringfencing** — Critical applications should only communicate with explicitly allowed parties. Internal application communications will be allowed.
- **Application microsegmentation** — Internal and external traffic of critical applications will only be allowed if explicitly approved (Zero Trust).
- **"Off corporate" endpoint segmentation** — The attack surface of an endpoint outside the protection of a corporate network will be limited. Akamai Guardicore Segmentation enables different rulesets for on and off your corporate network.
- **Privilege access to servers** — Server access control policy can be implemented, for example, to restrict management ports to jump boxes only or to prevent access to specific servers based on user identity of the source.
- **Security best practices enforcement** — Block list rules will be implemented to enforce network security best practices.

Implementation Engineer

When an enterprise requires a significant number of policy objectives, it is often preferable to work with an assigned engineer for a set period with no limits on the number of policies our engineer can create for you to ensure successful implementation. Allowing Akamai to provide the implementation support you require to achieve your goals is ideal when your network needs full end-to-end segmentation.

	Jumpstart	Extended Jumpstart	Implementation Engineer
Installation	✔	✔	✔
Installation of labeling schema	✔ Limited	✔ ✔ ✔	Comprehensive implementation resources for a set period, with no limitations on use cases, ensuring your success goals are met
Guidance on overall security posture	✔ Limited	✔ ✔ ✔	
Guidance on policy creation	✔ Limited	✔ ✔ ✔	
Implement policy use case(s)	**Single policy**	**Multiple policies**	
End-user training	✔	✔	✔
Typical duration	**6 months**	**12 months**	**6-18 months**
When to choose which option	Customer or partner prefers to implement mostly in-house; Akamai implements only first use case	Akamai implements multiple use cases, multiple policies, and extensive guidance	Customer or partner wants full implementation (multiple use cases), prefers to explore and define exactly what and how throughout the period

Akamai training

Akamai certification training for microsegmentation equips administrators (GCSA) and operational engineers (GCSE) with the necessary skills and information required to succeed at their related maintenance and administrative tasks.

Training methods are versatile to meet customers' and partners' needs: from basic online training to instructor-led certification training and even private, dedicated (virtual or in-person) training.

Guardicore Certified Segmentation Administrator (GCSA)

Our program of five half-days equips users of the Akamai Guardicore Segmentation platform with the expertise required to successfully operate all aspects of the platform. GCSA graduates will gain the confidence to use the platform by themselves to implement and maintain their organization's security needs.

The course covers Akamai Guardicore Segmentation's core feature set: visibility, labeling, microsegmentation, and breach detection. The focus is primarily on feature behavior and usage, and the course will guide students from the initial configuration of Akamai Guardicore Segmentation all the way to common day-to-day operations.

Guardicore Certified Segmentation Engineer (GCSE)

Our program of three half-days equips the operational owners of the system with the skills and knowledge required to perform platform-related administrative and maintenance tasks.

GCSE graduates will be able to manage the overall operation of the Akamai Guardicore Segmentation environment. The course covers the following topics: platform and components configuration, integration with third-party tools, platform health checking, troubleshooting, and common maintenance tasks.

Both courses are accompanied by an online, hands-on lab that is available for all students for the duration of the course. A certification exam is held at the end of each course.

Enterprise Support and Customer Success

Our Enterprise Support program is designed to support all possible consequences of using Akamai Guardicore Microsegmentation in your organization. Our support organization will cover you 24/7/365, handle any support case you encounter, and assist you with upgrades and fixes.

Our Customer Success program helps you achieve your organization's short-term and long-term security goals while maximizing the value of the investment you've made in our platform.

Elite Support

Akamai's Elite Support provides your organization with priority access to designated, experienced, top-tier escalation experts. A highly skilled specialist, familiar with your data center and internal processes, will be your single point of contact and will help you expedite the response and resolution of any issue and will maximize your investment in software-based segmentation.

	Premium	Elite
Support availabilty	**24/7/365**	**24/7/365**
Unlimited cases	✔	✔
Upgrades and fixes	✔	✔
Phone, email, Slack, and portal	✔	✔
Root cause analysis (upon demand)	**Severity 1**	**Severity 1 & Severity 2**
Priority case handling by a designated experienced engineer		✔ Designated engineer available during business hours
Proactive and continuous system health monitoring		✔
Personalized optimization		✔ Quarterly optimization session
Periodic issue review and support report		✔ Weekly issues review; monthly support report
Consultation days		✔ 2, 4, or 6 consultation days per year depending on size (SKU)
When to choose which option	Smaller deployment; mainly needs support	Larger deployment; requires higher control on ongoing issues

Day-2 Operation Services

After deploying the first few use cases, customers reap value from the Akamai Guardicore Segmentation product. However, there is a need for ongoing maintenance and updates to maximize the value that can be gained from our product:

- Update deployment (assets, labels, policies) to reflect changes to the organization as they occur
- Implement additional use cases that were not handled during the initial deployment phase (new use cases you've identified now that you use our product, additional services and/or applications to handle, etc.)
- Implement Akamai Guardicore Segmentation on additional departments within your organization; e.g., cloud-based networks and applications. (either new or simply those left for phase 2)
- Deploy to additional endpoints, Internet of Things devices, virtual desktop infrastructure environments, etc.
- Use Akamai Guardicore Segmentation to identify and mitigate security events (i.e., stop lateral movement in your network); you can connect your environment to the Akamai Security Operations Command Center and get 24/7/365 monitoring and real-time alerting and mitigation
- Get enhanced, proactive, security via Akamai Hunt, Akamai Edge DNS (for secure DNS and protection against distributed denial of service), and Akamai Enterprise Application Access (for access and identity management)
- Use Akamai Guardicore Segmentation to assist you with your certification audits

These services should be provided by GcSP certified partners

Technical Account Managers and Resident Engineers

Akamai Technical Account Managers and Resident Engineers are senior technical advisors for enterprises with wide and potentially complex segmentation needs. Once embedded into your organization, our engineers quickly become experts in your environment, allowing you to achieve superior success with Akamai Guardicore Segmentation.

The Resident Engineer* assigned to your account will be embedded in your teams and will proactively support all your operations to ensure you gain the maximum value out of Akamai Guardicore Segmentation at all times.

The Resident Engineer can ensure your success by guiding you on policy decisions, informing you of the latest upcoming features in our product, planning (and assisting in executing) an upgrade, and performing executive business reviews.

Your Technical Account Manager or Resident Engineer can also supervise and execute your Day-2 Operation Services.

**The Resident Engineer may be remote*

Akamai Hunt: A managed threat hunting service

Akamai Hunt, an extension of Akamai Guardicore Segmentation, is our managed threat hunting service that can help you stay ahead of the most evasive threats and better protect your organization.

The Akamai Hunt team continuously hunts for anomalous attack behavior and advanced threats that consistently bypass even the most cutting-edge security solutions. With Hunt, you are notified immediately about any critical incidents detected in your network, and our experts work closely with your team to remediate any compromised asset for a fast resolution.

Whether you are focused on detecting and preventing ransomware, defeating advanced persistent threats, protecting against zero-day vulnerabilities, or improving your general IT security hygiene, Akamai Hunt allows you to get the most security value from your Akamai Guardicore Segmentation deployment without any additional software, agent rollouts, or upgrades.

Akamai Hunt includes:

24/7 expert human analysis — Our cybersecurity professionals come from a wide range of fields, including security research, offensive security, military intelligence, red team, incident response, and data science.

Alerts on real threats — To avoid alert fatigue, the Hunt team only alerts its customers about real threats, completely avoiding false positives.

Proprietary hunting tools — Akamai Hunt experts routinely develop advanced threat hunting algorithms — such as user and network activity anomalies, executable analyses, log analyses, and more — to form a powerful toolset for fast detection and response. Akamai Guardicore Insight, a powerful OS query–based tool to query endpoints and servers in real time, is included with the service at no additional cost.

Context-rich threat intelligence — Our team of Hunters collects indicators of compromise — from IPs and domains to processes, users, and services — by leveraging Akamai Guardicore Segmentation and the massive global threat intelligence of Akamai.

Network, cloud, and endpoint visibility — This combination of data generated from Akamai Guardicore Segmentation deployments and Akamai's global sensors — including more than 7 trillion daily DNS requests made to the Akamai DNS cloud — provides our team with the most comprehensive visibility of your environment.

Immediate notification and proactive insights —

- Email notifications are sent immediately after a threat is detected
- Periodic executive-level threat reports include analysis, stats, and metrics to keep your executives or board informed of the high-profile attack campaigns
- Incident management is easy with the integration of the Akamai Guardicore Segmentation console

To learn more about Akamai Guardicore Segmentation, visit akamai.com