eBPF In Production

An Overview of Compelling Enterprise Outcomes Using eBPF

by Bill Doerrfeld

February 2026

Contents

Executive Summary

eBPF has reached a new level of maturity as a production-grade infrastructure technology, delivering measurable improvements in performance, security, and operational efficiency across some of the world's largest and most complex systems. To that end, we've consolidated some of the world's leading examples of eBPF in production and their quantifiable results.

Designed for executive and senior technical leaders, **this paper focuses on tangible outcomes, cost reduction, risk mitigation, performance improvements, and improved system efficiency,** rather than theoretical potential, and provides a roadmap for how eBPF can positively impact their operations and business at large.

eBPF In Production Report

An Overview of Compelling Enterprise Outcomes Using eBPF

eBPF has been described as a programmable window into the Linux kernel, which underpins virtually all modern software devices and 96% of web servers worldwide. eBPF stands to revolutionize IT infrastructure by enabling programs to safely run in the kernel space with extremely low overhead, strong safety guarantees, and the flexibility to meet modern application demands.

Today, in production environments, eBPF is the prime vessel to apply custom networking, security, performance, or observability features without needing to rewrite or update the Linux kernel. Embedded within solutions that enable packet routing, filtering, and load balancing, eBPF can drive better network performance, latency, and throughput. The visibility you gain from analyzing kernel behavior can unlock efficiency and optimization gains that equate to significant cost savings, and eBPF also arms infrastructure with more sophisticated malicious detection and response capabilities that user space tools can't reach.

Since it was first merged into the Linux kernel a decade ago, eBPF has unlocked the kernel's full innovation potential, bypassing the constraints of traditional Linux release timelines. It allows enterprises to implement cutting-edge functionality immediately, rather than waiting years for upstream updates.

eBPF is now the strategic platform of choice for infrastructure teams, well-supported by tech hyperscalers, infrastructure-as-a-service platforms, software-as-a-service offerings, innovative startups, and open source projects alike. And the engineering stories emerging today finally represent eBPF's true utility and promise within enterprise IT.

In this report, we'll spotlight compelling case studies from a number of credible companies currently using eBPF in production. We'll highlight the community's pragmatic efforts around eBPF in practice, and **show both how organizations are putting eBPF to work and the tangible business benefits they are gaining.**

The Invisible Engine of Modern Infrastructure

eBPF as an Enterprise Standard

Many organizations are already using eBPF, even if they don't realize it. As Linux has become the foundation of modern infrastructure, eBPF has quietly emerged as a standard mechanism for extending, observing, and securing systems at scale. Some of the world's most complex networked devices and distributed systems now rely on eBPF to boost their operations in meaningful ways. eBPF is being leveraged more than ever with proven, **measurable outcomes**.

Android provides one of the clearest signals of this maturity. eBPF is triggered within every boot of the world's most pervasive Linux-based operating system powering **nearly four billion devices**. On Android, eBPF collects useful kernel-level statistics, aids memory profiling to fine-tune CPU, and optimize resource usage, strengthens security with runtime isolation, and more.

On the hyperscaler side, Google began implementing eBPF **as early as 2020** for both auditing and enforcing policies, greatly reducing friction compared to traditional kernel patching.

Google also **uses BPF** to handle a majority of their production traffic and programmatically adjust packet-based rate limits, improving scalability across massive traffic flows.

Similarly, Meta processes every packet entering its data centers through its eBPF-based **Katran** load balancer and uses eBPF-driven profiler **Strobelight** to reduce server requirements across critical services by double-digit percentages.

The list of large-scale eBPF adopters extends far beyond these tech giants. Major institutions across retail, finance, and media are deploying eBPF to modernize their infrastructure including Alibaba, Amazon, Apple, Capital One, eBay, IKEA, LinkedIn, Microsoft, New York Times, Samsung, Walmart, Wikipedia, and many others. This breadth of adoption confirms that eBPF is now a foundational component of the modern enterprise technology stack.

eBPF's Strategic Deployment Patterns

eBPF Aids Networking, Observability, Security, and Beyond

As eBPF adoption has expanded, consistent deployment patterns have emerged across industries. While eBPF is fundamentally a general-purpose kernel technology, enterprises tend to apply it first where traditional approaches struggle with performance, visibility, or operational friction. These common patterns represent the most immediate ROI. Let's distill these top uses through **eBPF case studies**.

High Performance Networking

Many organizations are using eBPF to make optimizations to how their networks operate. eBPF is actively applied in high-speed load balancing, high-performance packet processing, and routing. From accelerating service mesh to optimizing massive telecom dataplanes and making content-delivery networks (CDNs) more efficient, eBPF is at the forefront of more modern networking and advancing legacy networking approaches across both private and public clouds.

EXAMPLES

- **S&P Global**, **Ikea**, **Sky**, **Alibaba**, **Red Hat**, and **Wildlife Studios** use Cilium for networking.
- **Line Corp**, **The New York Times**, **Walmart**, **Yahoo**, **Seznam**, **Trip.com**, and **Wikimedia Foundation** apply eBPF for load balancing.
- Meta's **eBPF-based Katran** load balancer processes every packet into their datacenters.
- **Digital Ocean** uses eBPF to rate limit internal services.
- **Bell Canada** leverages eBPF for SRv6 modernization.
- **ArvanCloud** applies eBPF for CDN routing.
- **free5GC** reduces Kubernetes data plane latency with eBPF.

Deep Observability & System Intelligence

Traditional monitoring often requires heavy code instrumentation. eBPF "hooks" into the kernel to surface granular data, such as cross-zone latency and memory profiling, without requiring code changes. Many organizations use this deep visibility to inform systems tracing and debugging, aid GPU profiling, and CPU and memory management among other areas. This leads to optimizations that keep complex distributed systems leaner and more resilient.

EXAMPLES

- **Google** uses eBPF for auditing and performance monitoring.
- eBPF aids memory profiling on **Android**.
- **Netflix** gains network insights at scale via eBPF.
- **Polar Signals** observes cross-zone traffic with eBPF.
- **Palantir** uses eBPF to debug network problems.
- **Cruise** and **DigitalOcean** monitor GPU performance with eBPF.

- SaaS applications like **Datadog**, **groundcover**, **Odigos**, **Traceable**, and **Attribute** use eBPF to monitor application performance.
- **Isovalent** and **Canopus** offer observability platforms built on eBPF.
- **LinkedIn** uses an eBPF-based agent, Skyfall, for infrastructure observability.

Runtime Security and Policy Enforcement

Through eBPF, access to root-level signals and the ability to enforce policies within the kernel can boost cybersecurity efforts significantly. eBPF aids forensics to help detect intrusions and malware, and even limit certain workloads or block malicious actions in real-time. Organizations can enforce policies at runtime and verify behaviors, like LLM security or software supply chain integrity at scale. In practice, this shifts security from reactive analysis to preventative enforcement.

EXAMPLES

- eBPF is used within runtime security platforms like **SentinelOne**, **Aqua Security**, **Oligo Security**, **RAD Security**, **ThreatX**, **Upwind Security**, **Cycode**, **Kodem**, **Wiz**, and **Exein**.
- **Shopify** and **Apple** use eBPF for monitoring and intrusion detection.
- **DoorDash**'s BPFAgent enables kernel-level monitoring.
- **Capital One**'s internal platform uses Cilium for cloud security policies.
- **Ant Group** uses eBPF in its cloud native security platform.
- **Core Tech** leverages eBPF for DDoS mitigation.
- **FlowSecurity** uses eBPF for data-in-motion monitoring.
- **Microsoft** enhances Kubernetes process inspection with eBPF.
- **Sysdig** applies eBPF for system call tracing, forensics, and more.

Application Governance and FinOps

Since eBPF runs in the kernel and can see everything happening on a host, it can play a unique role in areas such as application programming interface (API) discovery, API observability, auto-instrumentation, and cost attribution. Tools are being developed that use eBPF under the hood to advance areas like understanding API behaviors, discovering shadow or zombie APIs, and attributing infrastructure costs to specific teams or services. This pattern is emerging but anticipated to grow as enterprises adopt agentic AI workflows and API-first architectures.

EXAMPLES

- **Levo**'s eBPF sensor aids API discovery to reduce sprawl.
- **Qpoint** adopts eBPF to monitor traffic to external APIs.
- **Traceable** enhances data collection with eBPF.
- **Akto** deploys eBPF when monitoring API traffic.
- **Attribute** uses eBPF programs to unlock cost visibility and attribution.

Key Business Results of eBPF in Production

Across a variety of use cases, industries, and business challenges, eBPF is already delivering strong ROI for organizations. Many companies have publicly quantified their use of eBPF as directly reducing costs, optimizing their infrastructure footprint, and leading to a measurable decrease in attacks. Let's review some of the impressive benchmarks that these organizations have shared over the years.

Reduced Infrastructure Costs

With deeper visibility into system and network behavior thanks to eBPF, organizations are enacting optimizations to boost usage efficiencies across CPUs and GPUs to improve utilization and streamline network activity. In some cases, these optimizations lead to substantially lower infrastructure spend.

- **Datadog** reports its **CPU usage dropped by 35%** through the use of an eBPF-based connection tracker.
- **Meta**'s Strobelight used eBPF to **reduce CPU cycles by up to 20%**.
- **Upwind**'s eBPF-based sensors are highly efficient, with **CPU usage less than 1% on average** and many nodes at **less than 0.1%** CPU utilization.
- **Polar Signals reduced operational costs related to cross-zone traffic by 50%** using in-house developed eBPF-based technology.

Increased Operational Efficiency and Scale

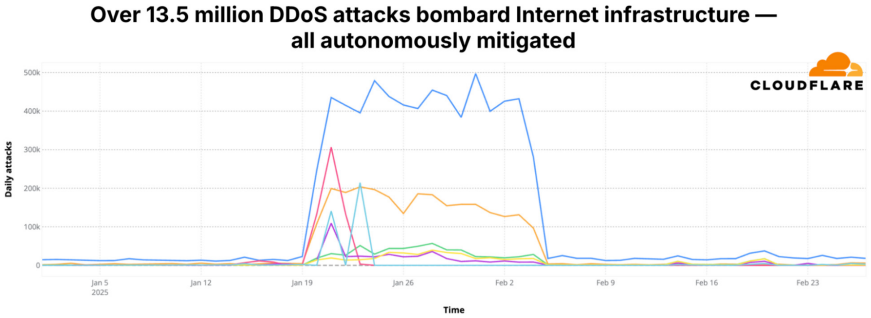
eBPF-based solutions bypass the heavy "tax" of user-space context switches and excessive data movement, leading to decreased call volumes, slimmer data streams, and faster deployment windows, enabling leaner and more scalable operations.

- **LinkedIn** reports its eBPF-driven infrastructure observability agent led to a **70% reduction in Kafka log volume**.
- **SuperNetFlow**'s network observability tooling used eBPF to achieve a **3x reduction in server footprint**.
- **Free5gc** achieved a **40% reduction** in highest round-trip time (RTT) using eBPF-based scheduling.
- **Seznam.cz doubled their throughput** while also **reducing CPU usage by 72x** using eBPF for load balancing.
- **DoorDash** migrated to eBPF-based monitoring to achieve **40% less memory, 98% fewer restarts, 80% faster deployment**, and **0.3% node utilization**.

Risk Mitigation and Attack Prevention

In the security domain, ROI is measured in prevention. eBPF-based solutions are used to detect and quickly mitigate anomalies, like denial of service (DDoS) attacks or suspicious actions. Fast reactions can reduce the financial risks caused by breaches, including the unauthorized usage of computing resources, high regulatory fines in the case of data leakage, and the loss of customer trust.

- **SentinelOne** uses an eBPF-based CWPP architecture to detect and stop real-time ransomware attempts in **under one second**.
- **CoreTech**'s scrubbing capability, powered by eBPF-based XDP, **successfully mitigated a DDoS attack that peaked at one terabyte per second** without incurring any downtime.
- **Crowdstrike** uses eBPF in its Falcon sensor agent for real-time monitoring of microservices, APIs, and SaaS applications.
- **Cloudflare**'s use of eBPF within XDP was instrumental in blocking a massive DDoS attack of **3.7 terabytes in just 45 seconds**.



- **Meta** adopted eBPF to enforce system-wide mandatory access control through its BpfJailer framework.

Improved Developer Velocity and Reduced Friction

While less quantifiable with independent ROI statistics, it should be noted that eBPF-based platforms can boost developer experience and reduce friction for security and platform engineers. By centralizing policy enforcement and observability at the kernel level, teams spend less time maintaining instrumentation, troubleshooting blind spots, and meeting organizational and industry-specific compliance.

For instance, Capital One made policy enforcement more achievable across teams with its eBPF-based platform using Cilium. As Capital One's Bradley Whitfield **shared in a 2020 lightning talk:** "This stack has allowed us to provide **less friction to even more and more teams**, while using modern technology to meet our security and regulatory requirements."

A Closer Look at Enterprise eBPF Wins

eBPF is already at the core of countless worldwide networks that serve billions of users, helping large organizations to observe low-level signals, optimize customer experience, lower costs, and reduce risk. Let's zoom in on four case studies that exemplify the utility of eBPF in practice, and how these large companies are receiving an ROI from using eBPF as a foundation for their infrastructure.

Cloudflare

eBPF AS THE BACKBONE OF A SAFER, FASTER INTERNET

Cloudflare operates one of the world's largest global networks, serving more than 200,000 customers, including over **a third of the Fortune 500**, and proxying traffic for **roughly 20%** of all websites. At this scale, infrastructure efficiency and security are existential concerns. eBPF has become a **core building block** underpinning Cloudflare's networking, observability, and security capabilities. A bulk of the world is, in effect, already reliant upon eBPF.

> *"Our usage of eBPF gives us the ability to maximize the flexibility of our systems, run our systems efficiently, improve our security, and monitor more deeply"*
>
> – Chris Arges, senior systems engineer at Cloudflare

"Our usage of eBPF gives us the ability to maximize the flexibility of our systems, run our systems efficiently, improve our security, and monitor more deeply," says Chris Arges, senior systems engineer at Cloudflare. "Our usage at Cloudflare has been primarily networking related," he adds. "This includes our ability to develop technology that can mitigate denial-of-service (DDoS) attacks as well as allowing for more efficient intra-datacenter load balancing."

eBPF is pervasive behind the scenes at Cloudflare, utilized in many areas, from **DDoS mitigation** to **load balancing**, **monitoring** their vast fleet of servers, and more. To do so, Cloudflare deploys several eBPF programs in production:

- eXpress Data Path (XDP), for handling traffic before it even hits the host
- Traffic classifier, for classifying and filtering network packets
- **Socket-level BPF**, which allows policy enforcement or redirection in the kernel
- **Linux Security Modules** (LSM), a hook-based framework to create security policies
- Tracepoint programs that measure specific kernel events

One effect of eBPF has been reducing risks like privilege escalation within their core systems. "By hooking into Linux Security Modules, we were able to use eBPF to improve our security programmatically and gain more flexibility," says Arges.

Another result has been more fine-grained observability. As Arges shares: "Our metrics use case was super-powered using eBPF." Writing for the **Cloudflare blog**, Ivan Babrou shares how Cloudflare's open source **ebpf_exporter** safely retrieves high-resolution kernel-level metrics, which can be applied to help detect incidents, decrease mean time to repair, and lower customer-facing latency.

Cloudflare, a company known for its engineering transparency and work in open source, also regularly shares its advances with eBPF with the broader cloud native community and contributes to the upstream project. “Cloudflare has been using eBPF for a long time, and not only have we embraced it across our infrastructure and products, but we’ve also improved it with new features and bugfixes,” adds Arges.

By standardizing on eBPF across teams and use cases, Cloudflare has reduced operational complexity while continuing to scale performance and security in parallel.

Cloudflare Reaps Business Benefits Using eBPF:

- **Terabit-Scale Defense:** Successfully mitigated attacks peaking above 7 Terabits per second (Tbps) without service degradation.
- **Faster issue detection:** Find and mitigate problems earlier
- **Lower operating costs:** Run systems more efficiently
- **Stronger security:** Flexible policies harden core systems

Netflix

eBPF HELPS OPTIMIZE MASSIVE USER-FACING INFRASTRUCTURE

The streaming giant Netflix has integrated eBPF into a range of critical areas, including performance tooling, compute, network observability, and low-latency infrastructure. These efforts have delivered tangible optimizations across their platform, helping them better serve over 325 million paid subscribers worldwide.

“By embedding eBPF into our systems, we’ve gained the ability to collect detailed real-time telemetry and optimize resource usage without requiring disruptive changes to application code,” says Anjali Kanak, senior engineering manager, Netflix, leading the application networking organization. “This technology has proven especially significant in enabling us to fine-tune system behavior at scale, supporting rapid innovation and operational reliability across our platform.”

> *“eBPF has proven especially significant in enabling us to fine-tune system behavior at scale, supporting rapid innovation and operational reliability across our platform”*
>
> – Anjali Kanak, senior engineering manager at Netflix

A major area of impact has been network defense. eBPF-based XDP programs help Netflix mitigate malicious traffic at the network interface level, bypassing costly user-space processing. “This enabled rapid, low-overhead DDoS mitigation, preserving compute resources for legitimate streaming and live event traffic while also improving blocking efficiency by orders of magnitude,” says Netflix’s Kanak.

Netflix engineers have also used eBPF to diagnose "noisy neighbor" issues, which are when a container heavily utilizes a shared server's resources. Netflix found that container latency can jump from 83µs to 131ms when a noisy neighbor appears. With eBPF's low-overhead instrumentation, they can detect this instantly and trace the source and remediate before customer-facing impact. eBPF flow logs have also helped Netflix handle a huge volume of observability data.

Community-driven projects have been essential to Netflix's overall journey with eBPF. "Leveraging the knowledge and tools from the open source community has been invaluable in accelerating progress and avoiding common pitfalls," adds Kanak. "In the context of the compute team, we rely on the **Cilium** eBPF library for Go, which has enabled us to embrace eBPF from our preferred development environment."

So far, Netflix's rollout of eBPF has been deliberate and focused on high-impact use cases. "One of the key lessons from our adoption journey is the importance of starting with well-defined, high-impact use cases, which allows teams to build confidence and expertise incrementally," says Kanak.

And in the next few years, eBPF's role at Netflix is expected to grow. "There is strong potential to expand the use of eBPF for additional networking and compute solutions at Netflix as our systems continue to evolve," Kanak, who adds they are exploring **netkit** for container networking.

"We are excited by the ongoing innovation in the eBPF ecosystem and expect it will remain a key enabler for building scalable, efficient infrastructure," says Kanak. "Across the tech industry, eBPF is likely to remain prominent as organizations look for ways to gain deeper visibility, control, and flexibility in their platforms."

"We are excited by the ongoing innovation in the eBPF ecosystem and expect it will remain a key enabler for building scalable, efficient infrastructure"

- Anjali Kanak, senior engineering manager at Netflix

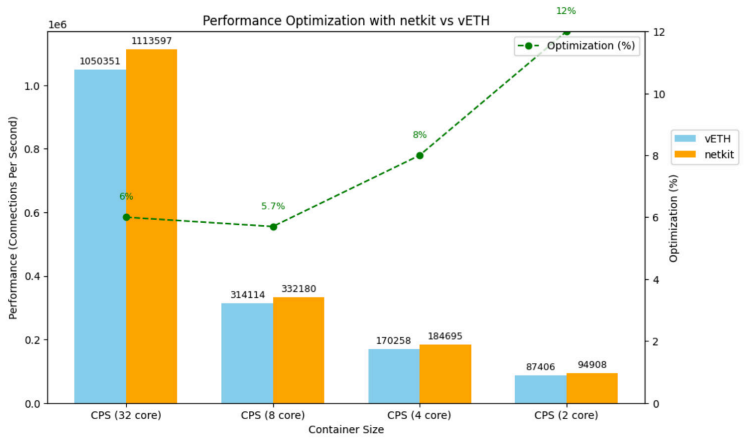
Netflix Gains An Edge With eBPF:

- **Reduced costs:** Optimize heavy resource usage
- **Empowered innovation:** Deep observability enables rapid iteration
- **Better customer experience:** Stronger security and multi-tenant reliability

ByteDance

eBPF NETWORKING AT BILLION USER SCALE

ByteDance is known for developing the video-sharing platform TikTok, which services an estimated 1.5 billion users worldwide. To improve performance across its massive infrastructure, the company has increasingly **turned to eBPF**.



ByteDance's large footprint is powered by roughly one million servers running containerized applications, which faced bottlenecks and stability concerns using traditional veth networking. To optimize performance at scale, ByteDance is **migrating its servers** to an eBPF technology called **netkit**, a kernel-native network device designed for eBPF networking programs.

> *"eBPF is the most important tool for us to work with the Linux kernel"*
>
> - Chen Tang, cloud computing developer at ByteDance

"eBPF is the most important tool for us to work with the Linux kernel," says Chen Tang, cloud computing developer, ByteDance. Tang is involved in building ByteDance's self-developed container networking interface (CNI) for their Kubernetes clusters. "We mainly use eBPF for container networking, like Cilium." Using netkit, ByteDance saw a 10% improvement in throughput. The migration required several engineering efforts, including backporting to earlier Linux kernel versions to match internal baselines and preparing fallbacks for unexpected behavior. Still, the benefits outweigh the challenges.

"I'm confident to say that netkit is trustable," shared ByteDance's Tang at the **eBPF Summit in 2024**. "We are motivated to widely deploy netkit in our datacenters." The move to netkit has also unintentionally resolved several long-standing issues with veth, such as high CPU consumption and certain packet disorder problems.

Looking ahead, ByteDance expects **its use of eBPF** to continue expanding. "We are also trying to explore eBPF for hardware offloading to save more CPU resources," says Tang.

ByteDance Proves eBPF Brings Key Advantages:

- **Decreased latency:** Across one million servers
- **Reduced costs:** Lower CPU usage and waste
- **Improved user experience:** More stable, predictable networking

Rakuten

eBPF POWERS TELCO MODERNIZATION

Rakuten is a global technology conglomerate based in Japan that operates many lines of business, including Rakuten Mobile, a mobile network operator unique for its decentralized cloud native infrastructure. **eBPF plays a central role in Sauron**, Rakuten Mobile's in-house platform for securing and monitoring its large hybrid network environment.

Sauron uses eBPF across three major categories:

- **Transport:** eBPF enables active network monitoring across network types, including end-to-end and hop-by-hop latency, jitter, packet loss, and QoS. This informs AI agents to detect anomalies.
- **Observability:** eBPF provides virtual tapping and packet extraction on any virtual interface. eBPF-enhanced monitoring approaches lead to fewer dropped events and fewer runtime failures.
- **Security:** eBPF enriches root-cause analysis with granular visibility into system calls, process behavior, and security signatures, helping teams pinpoint issues quickly and precisely.

"eBPF, through the Sauron platform, has transformed Rakuten Mobile by strengthening anomaly detection and security in our cloud native telecom networks, directly contributing to risk mitigation and improved operational visibility and control over network performance and security," says Dr. David Soldani, SVP innovation and advanced research at Rakuten, and CISO of Rakuten Symphony.

From an operations standpoint, eBPF has also delivered strong efficiency gains. "eBPF-mirrored detection significantly reduces CPU use and latency, making it much more efficient under load," says Rakuten's Soldani. Even at very high throughput and large packet sizes, maximum total CPU utilization is around 20% of one core, he adds.

As an innovative telecommunications provider, Rakuten Mobile is exploring how eBPF can support next-generation AI/ML capabilities. As Soldani describes, his team is currently working on eBPF intelligent agents for real-time AI inference, observability, performance monitoring, and security tooling.

All in all, eBPF has delivered quantifiable impacts to Rakuten Mobile including reduced mean time to detect (MTTD) and mean time to resolve (MTTR) for network and security incidents, a decrease in security breaches, increased network performance leading to higher customer satisfaction, reduced churn, and lower operational costs.

Looking to the future, Soldani expects Rakuten Mobile's use of eBPF to evolve further. This includes more sophisticated AI/ML use cases, expanded automation for policy enforcement, and continued refinement of Sauron's anomaly detection and security features. He also sees broader use of eBPF at Rakuten Mobile beyond its mobile communication network.

> *"eBPF-based workflows will be instrumental in defining and implementing granular runtime security controls and monitoring capabilities in O-RAN and 6G"*
>
> – Dr. David Soldani, SVP innovation and advanced research at Rakuten, and CISO of Rakuten Symphony

For these reasons and more, eBPF is poised to benefit emerging technology standards within Rakuten and telecommunications at large. “eBPF-based workflows will be instrumental in defining and implementing granular runtime security controls and monitoring capabilities in O-RAN and 6G,” Soldani finishes.

Rakuten Taps eBPF To Harden Cloud Native Security:

- **Quicker response:** Reduced time to resolve and fewer incidents
- **AI-enablement:** Granular data for advanced anomaly detection and remediation
- **Lower overhead:** Reduction in compute costs for observing events

eBPF as the Future of Infrastructure Software

Countless Enterprises Report Gains From eBPF

The takeaway for leaders is clear: **eBPF is already woven into the fabric of modern, large-scale distributed systems.** In fact, any modern Linux kernel already includes eBPF, and organizations deploying eBPF report consistent gains in performance, efficiency, and security backed by production data at global scale.

Results of applying eBPF across areas like networking, observability, and security are apparent and the differentiation now lies in how organizations strategically leverage it to gain competitive advantages in speed, security, and cost efficiency. Reduced CPU cycles and higher network throughput translate directly into lower cloud costs. Detecting malicious behavior at the source curbs attacks. Granular kernel-level visibility into latency, errors, and system usage fuels more efficient tuning and operations.

Consumers of eBPF technology should no longer view these deployments as isolated wins in networking or security. Instead, they should view eBPF as a modular, extensible foundation. Networking, security, and observability are interrelated at the kernel level, where the building blocks used for one category naturally reinforce the others. **Organizations that treat eBPF as a unified infrastructure layer will realize the compound benefits of reduced overhead and unified telemetry.** And once deployed, many organizations forecast expanding their eBPF use into new areas in the near future to continue to leverage eBPF as their strategic infrastructure platform of choice.

Since the four organizations highlighted as the main case studies in this report have all benefited from the eBPF community in some way, their stories are also a testament to the passion and collaboration within the eBPF community. As a steward of the eBPF community, the eBPF Foundation plays a critical role in accelerating discussions, highlighting interesting case studies and open source projects, and helping shape the next generation of infrastructure software with eBPF.

Bibliography

1. eBPF Foundation. (n.d.). eBPF case studies. **https://ebpf.io/case-studies/**
2. Android Open Source Project. (n.d.). Extend the kernel with eBPF. **https://source.android.com/docs/core/architecture/kernel/bpf**
3. DemandSage. (2024). Android statistics. **https://www.demandsage.com/android-statistics/**
4. Google. (2020). eBPF for auditing and policy enforcement [Video]. YouTube. **https://www.youtube.com/watch?v=XFJw37Vwzcc&t=657s**
5. Miranda, M. (2020). Replacing HTB with EDT and BPF. netdevconf. **https://netdevconf.info//0x14/pub/papers/55/0x14-paper55-talk-paper.pdf**
6. eBPF Foundation. (2024). Meta's Strobelight leverages eBPF to reduce CPU cycles and server demands by up to 20%. **https://ebpf.foundation/case-study-metas-strobelight-leverages-ebpf-to-reduce-cpu-cycles-and-server-demands-by-up-to-20/**
7. Cilium Project. (n.d.). Cilium. **https://cilium.io/**
8. FOSDEM. (2025). An introduction to netkit: The BPF programmable network device. **https://archive.fosdem.org/2025/schedule/event/fosdem-2025-4045-an-introduction-to-netkit-the-bpf-programmable-network-device/**
9. S&P Global. (2024). How S&P Global uses Cilium [Video]. YouTube. **https://www.youtube.com/watch?v=6CZ_SSTqb4g**
10. IKEA. (2024). IKEA's Cilium adoption [Video]. YouTube. **https://www.youtube.com/watch?v=sg-F_R-ZVNc**
11. Sky. (2023). Sky networking with eBPF [Video]. YouTube. **https://www.youtube.com/watch?v=u-4naOMfs_w**
12. Alibaba Cloud. (2023). How Alibaba Cloud builds high-performance cloud-native pod networks. **https://www.alibabacloud.com/blog/how-does-alibaba-cloud-build-high-performance-cloud-native-pod-networks-in-production-environments_596590**
13. Red Hat. (2023). Cilium networking at scale [Video]. YouTube. **https://youtu.be/xxRAppnmirY**
14. Wildlife Studios. (2020). Multi-cluster gaming platform with Cilium. **https://cilium.io/blog/2020/09/03/wildlife-studios-multi-cluster-gaming-platform/**
15. LINE Corporation. (2023). LINE + eBPF networking [Video]. YouTube. **https://www.youtube.com/watch?v=cxfVpBYlol4**
16. The New York Times. (2024). NYT's load balancing evolution [Video]. YouTube. **https://www.youtube.com/watch?v=qmrHONqsV2M**
17. Walmart Global Tech. (2020). Introducing Walmart's L3AF project. **https://medium.com/walmartglobaltech/introducing-walmarts-l3af-project-how-do-we-use-ebpf-to-provide-network-visibility-in-a-8b9ae4d26200**
18. Yahoo / USENIX. (2021). eBPF for load balancing. **https://www.usenix.org/conference/lisa21/presentation/jones-zachary**
19. Seznam.cz. (2022). Cilium standalone L4LB XDP. **https://cilium.io/blog/2022/04/12/cilium-standalone-L4LB-XDP/**
20. Trip.com Group. (n.d.). Trip.com. **http://trip.com**
21. Facebook Engineering. (2018). Katran: A scalable network load balancer. **https://engineering.fb.com/2018/05/22/open-source/open-sourcing-katran-a-scalable-network-load-balancer/**
22. DigitalOcean. (2022). Using eBPF for rate-limiting [Video]. YouTube. **https://www.youtube.com/watch?v=gcHxfhDT-I4**
23. Bell Canada. (2024). SRv6 modernization with eBPF [Video]. YouTube. **https://www.youtube.com/watch?v=fNtG0iHYne4**
24. Wikimedia Foundation. (2025). Papal announcement traffic surge incident. **https://wikitech.wikimedia.org/wiki/Incidents/2025-05-08_Papal_announcement_traffic_surge**
25. ArvanCloud. (n.d.). We removed shared memory by building an eBPF load balancer. **https://medium.com/@amiremohamadi/we-removed-shared-memory-by-building-an-ebpf-load-balancer-394f9f1b344**
26. free5GC. (2025). Reducing Kubernetes data plane latency with eBPF. **https://free5gc.org/blog/20250726/index.en/**
27. netdevconf. (n.d.). Replacing HTB with EDT and BPF. **https://netdevconf.info//0x14/session.html?talk-replacing-HTB-with-EDT-and-BPF**

28. Netflix. (2022). How Netflix uses eBPF flow logs. **https://netflixtechblog.com/how-netflix-uses-ebpf-flow-logs-at-scale-for-network-insight-e3ea997dca96**
29. Polar Signals. (2024). Cross-zone network traffic monitoring with eBPF. **https://ebpf.foundation/case-study-polar-signals-uses-ebpf-to-monitor-internal-cross-zone-network-traffic-on-kubernetes-reducing-these-operating-costs-by-50/**
30. Palantir. (2023). Debugging with eBPF [Video]. YouTube. **https://www.youtube.com/watch?v=0RDp1IPxbg0**
31. Cruise. (2023). GPU monitoring with eBPF [Video]. YouTube. **https://www.youtube.com/watch?v=7bdy2AkRjqE**
32. Datadog. (2024). Improving network observability with eBPF. **https://ebpf.foundation/case-study-datadog-uses-ebpf-to-improve-network-observability-accuracy-and-performance/**
33. groundcover. (2024). How groundcover uses eBPF [Video]. YouTube. **https://www.youtube.com/watch?v=73wait5RR7c**
34. Odigos. (n.d.). How Odigos uses eBPF. **https://odigos.io/blog/how-odigos-uses-ebpf**
35. Traceable. (n.d.). Unlocking the power of eBPF. **https://www.traceable.ai/blog-post/unlocking-the-power-of-ebpf-at-traceable**
36. Attribute. (n.d.). Unlocking cloud cost visibility with eBPF. **https://attrb.io/unlocking-cloud-cost-visibility-with-ebpf-a-game-changer-for-finops/**
37. Isovalent. (n.d.). Next-generation observability with eBPF. **https://isovalent.com/blog/post/next-generation-observability-with-ebpf/**
38. Canopus. (n.d.). SuperNetFlow eBPF case study. **https://ebpf.foundation/case-study-supernetflow-reinventing-network-observability-with-ebpf/**
39. LinkedIn Engineering. (2022). Skyfall: eBPF agent for infrastructure observability. **https://engineering.linkedin.com/blog/2022/skyfall--ebpf-agent-for-infrastructure-observability**
40. SentinelOne. (2023). The advantages of eBPF for CWPP applications. **https://www.sentinelone.com/blog/the-advantages-of-ebpf-for-cwpp-applications/**
41. Aqua Security. (2023). Linux vulnerabilities & Tracee. **https://blog.aquasec.com/linux-vulnerabilitie-tracee**
42. Oligo Security. (2023). Scaling runtime security with eBPF. **https://www.oligo.security/blog/scaling-runtime-security-how-ebpf-is-solving-decade-long-challenges**
43. RAD Security. (2024). Introducing RAD Security. **https://www.radsecurity.ai/blog/introducing-rad-security**
44. ThreatX. (2024). Cisco acquires Isovalent. **https://www.threatx.com/blog/cisco-acquires-isovalent-creator-of-ebpf-why-it-matters/**
45. Upwind. (n.d.). How Upwind uses eBPF. **https://www.upwind.io/feed/how-upwind-uses-ebpf-to-bring-real-time-security-to-cloud-native-environments**
46. Cycode. (n.d.). Introducing Cimon build hardening. **https://cycode.com/blog/introducing-cimon-build-hardening/**
47. Kodem. (n.d.). Comparing eBPF and kernel modules. **https://www.kodemsecurity.com/resources/comparing-ebpf-and-kernel-modules-for-application-vulnerability-detection-and-attack-monitoring**
48. Wiz. (n.d.). Wiz expands platform with runtime sensor. **https://www.wiz.io/blog/wiz-expands-platform-with-the-runtime-sensor-to-provide-unified-cloud-security**
49. Exein. (n.d.). Runtime security with eBPF [Video]. YouTube. **https://www.youtube.com/watch?v=vmRQXRit-sY**
50. Shopify. (2023). Falco for intrusion detection [Video]. YouTube. **https://www.youtube.com/watch?v=6pVci31Mb6Q**
51. Apple. (2023). Monitoring with Falco [Video]. YouTube. **https://www.youtube.com/watch?v=ZBlJSr6XkN8**
52. DoorDash Engineering. (2023). BPFAgent: eBPF for monitoring at DoorDash. **https://doordash.engineering/2023/08/15/bpfagent-ebpf-for-monitoring-at-doordash/**
53. Capital One. (2020). eBPF for cloud security policies [Video]. YouTube. **https://www.youtube.com/watch?v=hwOpCKBaJ-w**

54. Ant Group. (n.d.). Ant Group secures platform with Kata Containers & eBPF. **https://ebpf.foundation/ant-group-secures-their-platform-with-kata-containers-and-ebpf-for-fine-grained-control/**
55. CoreTech. (n.d.). How to drop 1 Tbps DDoS traffic. **https://www.linkedin.com/pulse/coretechnologys-how-drop-1-tbps-ddos-traffic-coretechnolgys-rayif/**
56. FlowSecurity. (n.d.). eBPF data-in-motion monitoring. **https://www.flowsecurity.com/ebpf-data-security-hype/**
57. Microsoft. (2024). Kubernetes process inspection with eBPF [Video]. YouTube. **https://www.youtube.com/watch?v=ilcYXPDSgu8**
58. Sysdig. (n.d.). Sysdig and Falco now powered by eBPF. **https://www.sysdig.com/blog/sysdig-and-falco-now-powered-by-ebpf**
59. Levo. (n.d.). API inventory with eBPF. **https://www.levo.ai/use-case/api-inventory**
60. QPoint. (n.d.). Tap into your egress traffic with eBPF. **https://www.qpoint.io/blog/tap-into-your-egress-traffic-with-ebpf/**
61. Akto. (n.d.). Traffic connector: eBPF. **https://docs.akto.io/traffic-connector/ebpf/ebpf**
62. LinkedIn Engineering. (n.d.). 2024 lightning talk (Capital One). **https://www.youtube.com/watch?v=hwOpCKBaJ-w**
63. Cloudflare. (2022). Cloudflare architecture and how BPF eats the world. **https://blog.cloudflare.com/cloudflare-architecture-and-how-bpf-eats-the-world/**
64. Cloudflare. (2024). Cloudflare named a Fortune Future 50 company. **https://www.cloudflare.com/press/press-releases/2024/cloudflare-named-a-fortune-future-50-company-ranked-14-on-2024-list/**
65. W3Techs. (2024). Cloudflare usage statistics. **https://w3techs.com/technologies/details/cn-cloudflare**
66. Cloudflare. (2022). L4Drop: XDP eBPF-based DDoS mitigations. **https://blog.cloudflare.com/l4drop-xdp-ebpf-based-ddos-mitigations/**
67. Cloudflare. (2022). Unimog: Cloudflare's edge load balancer. **https://blog.cloudflare.com/unimog-cloudflares-edge-load-balancer/**
68. Cloudflare. (2022). Introducing ebpf_exporter. **https://blog.cloudflare.com/introducing-ebpf_exporter/**
69. Cloudflare. (2022). Socket-level eBPF. **https://blog.cloudflare.com/epbf_sockets_hop_distance/**
70. Cloudflare. (2022). Live-patch security vulnerabilities with eBPF LSM. **https://blog.cloudflare.com/live-patch-security-vulnerabilities-with-ebpf-lsm/**
71. GitHub. (n.d.). ebpf_exporter. **https://github.com/cloudflare/ebpf_exporter**
72. Netflix Engineering. (2023). Noisy neighbor detection with eBPF. **https://netflixtechblog.com/noisy-neighbor-detection-with-ebpf-64b1f4b3bbdd**
73. GitHub. (n.d.). bpftop. **https://github.com/Netflix/bpftop**
74. Isovalent. (2024). Netkit: A new container networking paradigm for the AI era. **https://isovalent.com/blog/post/cilium-netkit-a-new-container-networking-paradigm-for-the-ai-era/**
75. Git.kernel.org. (n.d.). netkit source code. **https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/tree/drivers/net/netkit.c**
76. ByteDance. (2024). Using eBPF and netkit at scale [Video]. YouTube. **https://www.youtube.com/watch?v=0w788CqTp0c**
77. The New Stack. (2024). ByteDance to network a million containers with netkit. **https://thenewstack.io/bytedance-to-network-a-million-containers-with-netkit/**
78. eBPF Foundation. (n.d.). Rakuten Mobile adopts eBPF. **https://ebpf.foundation/rakuten-mobile-adopts-ebpf-to-strengthen-anomaly-detection-and-security-in-cloud-native-telecom-networks/**

About the Author

BILL DOERRFELD

Bill Doerrfeld is an independent tech journalist and editor. He contributes to leading enterprise IT publications and provides content, analysis, and consulting for technology companies. His work focuses on advancing conversations around fast-moving, state-of-the-art enterprise software technologies.

The **eBPF Foundation** was created to advance eBPF as an open, shared technology for programmable infrastructure. It brings together a cross-platform community of maintainers and organizations working upstream to evolve eBPF's capabilities while ensuring its safety, security, and performance. Foundation members collaborate on common technical priorities, security best practices, community development, and promotional opportunities supporting eBPF across kernels, operating systems, and enterprise environments. Find further information here: **https://www.ebpf.foundation**

Copyright © 2026 **eBPF Foundation**

This report is licensed under the **Creative Commons Attribution 4.0 International Public License**.