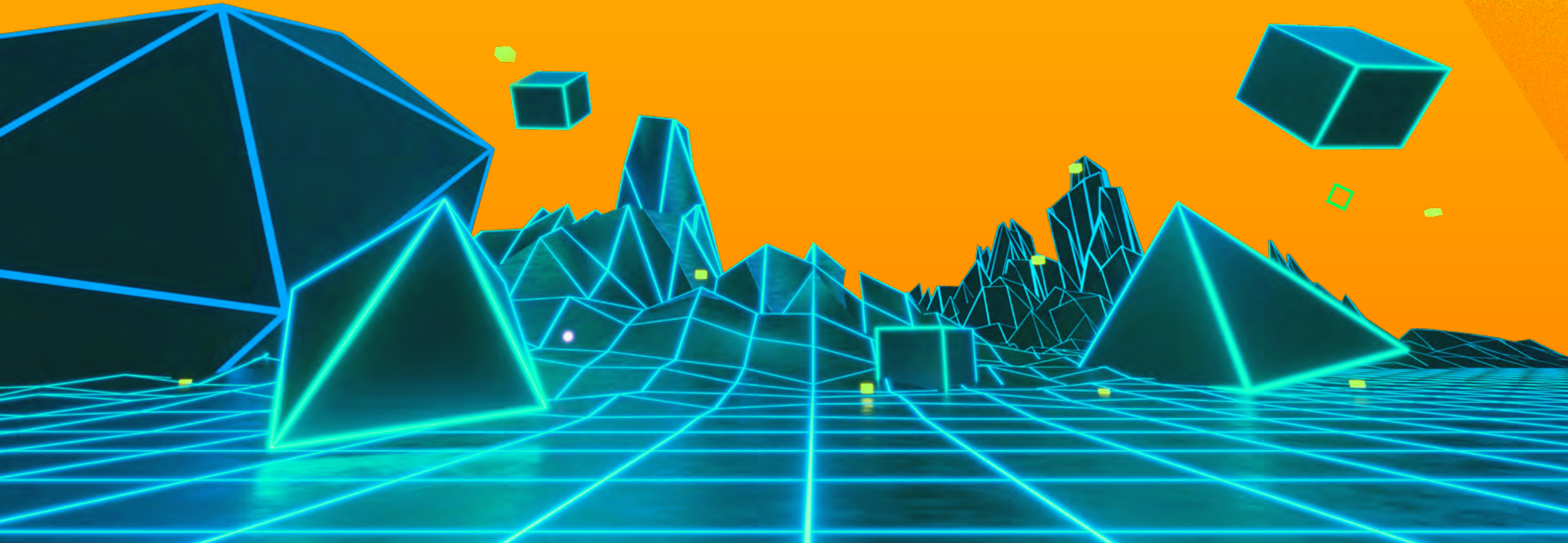
Cribl

EBOOK

2025 outlook for security and telemetry data

What's coming in the next year and how to prepare



CONTENTS

INTRODUCTION

How to navigate the future of telemetry data and security in 2025

The digital environment is evolving rapidly, bringing new challenges and opportunities to IT, Security, and compliance teams.

2025 will be a year marked by significant shifts in cybersecurity regulation, the rapid growth of observability technology, and the continued burdens of managing telemetry data in a world driven by artificial intelligence and cloud migration.

In this eBook, we explore for you the emerging trends and predictions that shape the future of enterprise IT and Security. From the global implications of the cybercrime convention to the pitfalls of failed AI projects, the insights we offer will help you prepare for what's ahead. We'll also examine the growing importance of telemetry data, the need for interoperability in observability solutions, and the seismic impact of recent legal decisions on cybersecurity regulation in the U.S.

Whether it's adapting to the loss of Chevron Doctrine protections or rethinking how we handle zombie AI data, these trends underscore the urgent need in telemetry data management for agility, strategic foresight, and open frameworks that keep pace with broad and rapid changes.

The future is complex, but it doesn't have to be overwhelming. Let's dive in and uncover the strategies you'll need to thrive in 2025 and beyond.

The cybercrime convention: A double-edged sword for enterprise security

The United Nations' adoption of the cybercrime convention marks a significant step to address the growing threat of global cybercrime. The treaty enhances international cooperation in preventing, investigating, and prosecuting cybercrimes with a framework for law enforcement agencies to work together across borders. However, this landmark agreement also raises concerns about privacy, data sovereignty, and potential implications for enterprise Security and IT teams.

The balance between security and privacy

While the cybercrime convention combats cyber threats, it also raises concerns about potential infringement of privacy rights. Provisions such as data retention and sharing requirements could increase surveillance and compromise individual privacy. While one country may consider some speech and activity legal or even protected, another may prohibit it. This delicate balance between security and privacy is a complex issue that will continue to shape the debates surrounding cybercrime and international cooperation.

Implications for enterprise security and IT teams

As organizations are increasingly interconnected and reliant on digital technologies, they must navigate a complex landscape of regulations and compliance requirements. The convention's provisions, combined with existing national and regional laws, can create a challenging operating environment for businesses.

Key challenges for enterprise security:

- **Data retention requirements:** The convention may require organizations to retain data for extended periods, increasing the burden on IT teams to manage and protect large volumes of data.
- **Cross-border investigations:** Businesses may face increased scrutiny from law enforcement agencies in multiple jurisdictions, requiring them to cooperate with investigations and potentially disclose sensitive information.
- **Cybercrime definitions:** The lack of universally agreed definitions of cybercrime can create challenges for organizations in understanding their obligations and complying with the law.
- **Technical challenges:** Implementing the necessary security measures to comply with the convention's requirements can be technically complex and resource-intensive.

Strategies for enterprise security teams:

- ✓ **Stay informed:** Keep up-to-date with cybercrime legislation and international regulations.
- ✓ **Assess compliance:** Thoroughly assess your organization's compliance with existing and emerging cybercrime laws.
- ✓ **Implement robust security measures:** Invest in strong security controls, including firewalls, intrusion detection systems, and encryption, to protect your organization's data and systems.
- ✓ **Develop incident response plans:** Create comprehensive incident response plans to effectively address cyberattacks and breaches.
- ✓ **Engage with law enforcement:** Build relationships with local law enforcement agencies to understand their expectations and requirements.

The road ahead

The cybercrime convention is a significant step in the global fight against cybercrime. However, its implementation will require a careful balance between security and privacy while posing challenges for enterprise Security and IT teams. By understanding the implications of the convention and taking proactive steps to address its requirements, organizations can better protect themselves from cyber threats and ensure compliance with international law.

The dark side of AI: Where does the data go when projects fail?

The AI landscape is a graveyard of ambitious projects. A staggering 80% of AI initiatives fail, according to a Rand study. That's a grim picture of the challenges inherent in AI development and deployment. But what happens to the vast amounts of data that fuel these failed projects?

Data swamps and compliance gaps

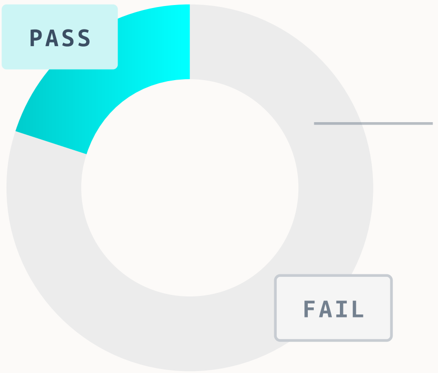
The rapid pace of AI innovation has outstripped the development of comprehensive regulations and compliance frameworks. This gap leaves an exploitable void for malicious actors. When AI projects fail, their data is often orphaned, creating data swamps that are vulnerable to breaches.

The dangers of zombie AI data

"Zombie" AI data is no longer actively used but remains accessible. It can be a treasure trove for hackers. Breaches involving zombie AI data can expose sensitive information with severe consequences for individuals and organizations.

Shining a light on the problem

Zombie AI data breaches draw significant attention to AI data management and may be a catalyst for stricter regulations and more robust compliance frameworks.



80%

of AI initiatives fail, according to a recent Rand study.

Key considerations for responsible AI development

To mitigate the risks of zombie AI data, organizations should:

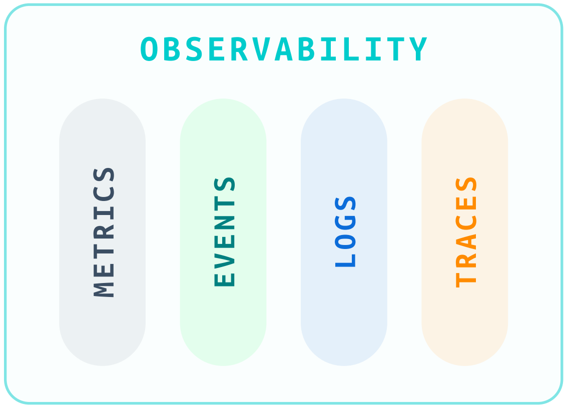
- **Implement robust data lifecycle management practices:** Include clear guidelines for data collection, storage, use, and disposal.
- **Prioritize data security:** Invest in strong security to protect data from unauthorized access and breaches.
- **Stay informed about evolving regulations:** Stay current with relevant data privacy and security laws.
- **Consider ethical implications:** Ensure that AI development and deployment align with ethical principles.

By addressing these issues, organizations can help to prevent the creation of data swamps and minimize the risks of zombie AI data.

Observability in 2030: A practitioner's wishlist

The return of Events in telemetry data

In the late 2010s, MELT was all the rage with vendors and practitioners extolling the virtues of Metrics, Events, Logs, and Traces as the "four pillars of observability," much to the chagrin of traces and logs purists. Confusion around the definitions of events and logs saw events slowly fade away, leaving the industry to argue about whether logs or traces were the best signal of them all.



The Four Pillars of Observability

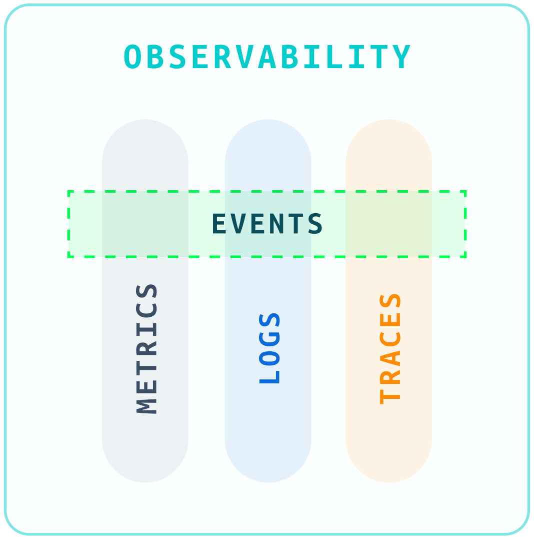
Of course we need metrics, logs, and traces

Everyone needs to have metrics as part of their observability strategy because they measure over time and answer, "Did something change?" It is when the answer is "Yes, something changed!" that we turn to logs and/or traces to answer, "What changed and who, or what, made the change?" In a full-stack observability strategy that includes containerized and monolithic workloads running across hybrid cloud, multi-cloud, and/or bare metal, your signal of choice is likely the logs. If you need to understand how applications responded when a metric indicates something changed, you need traces to tell the story.

But there is still a missing link. That is where events matter.

Don't miss Events

An event looks like a log entry, complete with a timestamp and a body of text, often with a source of the event, too. Events bring context to logs, metrics, and traces. That context can include a change to a system configuration, notifications of planned (or unplanned!) outages, product launches, even weather and geopolitical events. Events are essential to answering, "*Why does this change matter?*"—a question at the heart of reducing the volume of notifications that require response and limiting the cognitive load of an investigation.



Observability with Events for Context

Events = Context = Why

Metrics tell you that application latency increased. Logs, that there are no system errors. And traces, the specific container and calls that are impacted. It is events that give you the context that your product launch has gone viral and traffic has increased 100x on your platform (I bet you are glad you are running Kubernetes and your application is auto-scaling in response, too!).

Know the context, know the network

"In-context" is the Holy Grail of observability right now and "logs-in-context" is the most common phrase. "in-context" simply means that a shared context—an application, host, or something else—can be exploited for faster navigation between logs, metrics, and traces when you investigate issues. This is particularly useful when digging into the "unknown-unknowns," a key tenant of observability and one of the drivers for the current 28% CAGR for telemetry.

Essential context

The OpenTelemetry project includes a signal called resource, which stores attributes that describe the source of a log, metric, or trace for faster grouping and filtering. And, if the log and/or metric originated from an application, sharing the span and trace IDs unlocks a precise correlation between the measurement, the associated logs, and the code. This span and trace ID context is essential for distributed tracing because it allows observability across disparate systems with little to no common resource attributes. As containerization has expanded, the demand for distributed tracing has followed suit. But what about the network?

Lacking visibility

Navigating between signals emitted from the same set of entities is a well-known pattern and distributed tracing is the gold standard experience. While that satisfies the application layer and signals from across shared resources, to use the OpenTelemetry terminology, we still lack visibility into the network layer with similar context.

Proof of concept

Cross-Layer Telemetry, a project built by Justin Iurman, brings In Situ Operations, Administration, and Maintenance (IOAM) to OpenTelemetry to unlock visibility from L2 to L7. While RFC 9197 proposes the data fields and RFC 9378 proposes the deployment model, the Cross-Layer Telemetry project brings it all together in an amazing proof of concept.

Application and infrastructure collaboration

Chaining together network performance insights via CLT with a specific trace and span ID, gives deep network context to traces in an OpenTelemetry format. Discovering that intermediary network devices are causing performance degradation, as demonstrated in Iurman's demo video, will continue to break down the silos between application and infrastructure teams.

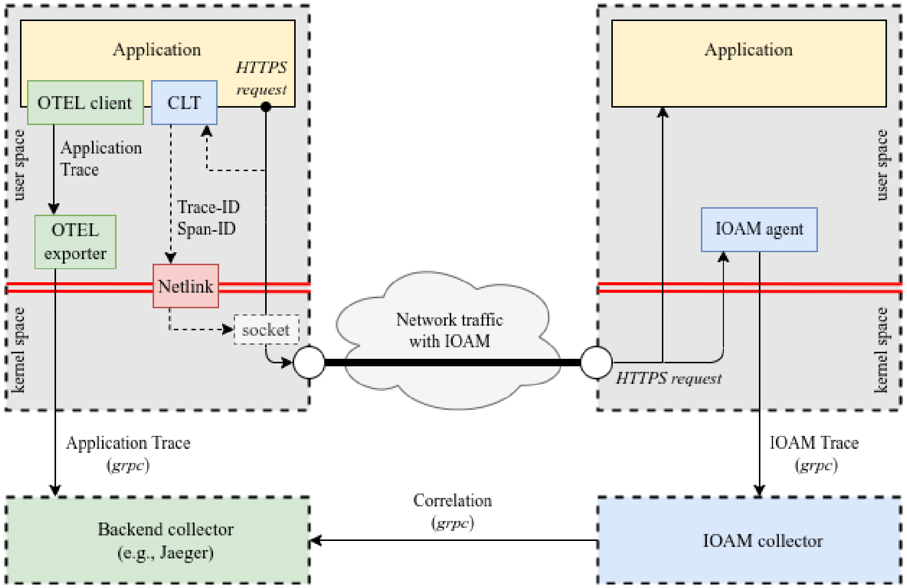


Image credit: Justin Iurman

Break the agent-analytics bond

The two previous hopes for 2030 involve new sets of telemetry—events from disparate sources, including events from outside the tech stack, and bridging the network-application divide. To achieve this new frontier of observability, we need to decouple the collection of telemetry from the analysis of telemetry.

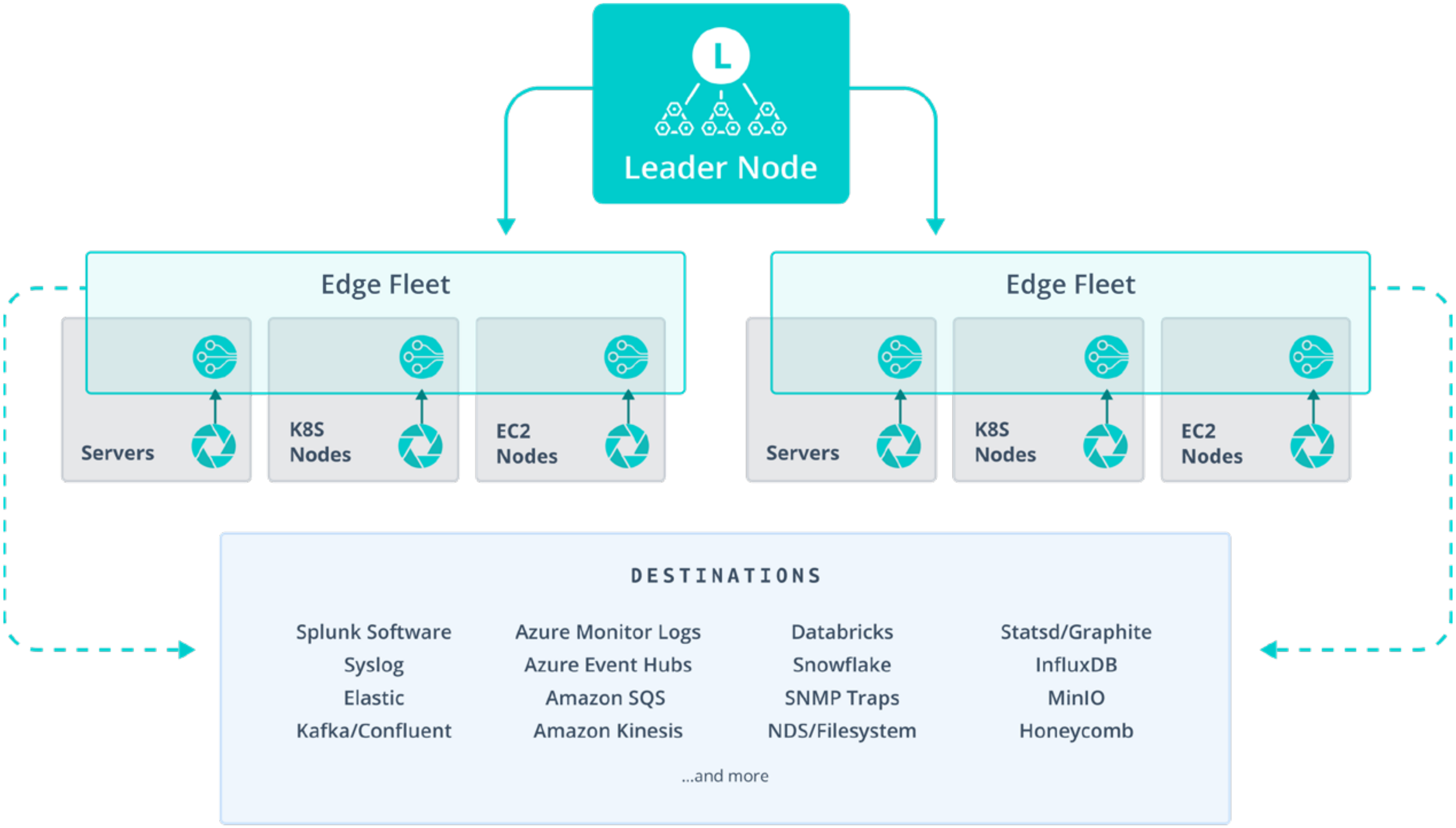
OpenTelemetry adoption will continue to advance and become the dominating signal format for application-centric observability. In addition, translating from non-OTLP to OTLP formats will become essential to using a single agent to power multiple experiences. Converting signal types will continue to dominate, with logs-to-metrics (and metrics from logs) and traces-to-metrics reducing the operational debt of multiple agents to power interchangeable tools to analyze, visualize, and correlate telemetry.

Treat your agents well

When choosing a backend for designing for observability, choose a solution that treats OpenTelemetry signals visualization and analysis with the same experience as their native agents. Swapping agents at the edge is an arduous task for enterprise-scale deployments, one that artificially impairs the adoption of new visualization and analytics experiences because of incompatible telemetry formats. In 2030, deploying a new agent should not be a prerequisite to deploying a new visualization experience or sharing the same telemetry set with multiple teams. Network flows for IT operations summarized as metrics and raw flows to both security and network operations should not require three different configurations.

Free your agents

Breaking down the barriers of telemetry across technologies and deployment models demands that we decouple agents from the platforms they power.



Here's an example of how a solution like Cribl Edge can help you centrally manage fleets of vendor-neutral agents to seamlessly adapt to evolving analysis tools.

Losing the Chevron Doctrine is a blow to US cybersecurity

Early in 2024, there was a webinar with key federal CISOs about the current state and future of federal cybersecurity. The looming *Loper Bright Enterprises v. Raimondo* decision from the U.S. Supreme Court (SCOTUS) regarding the Chevron Doctrine was largely unknown and ignored.

What is the Chevron Doctrine?

In June 2024, the SCOTUS ruling in *Loper Bright Enterprises v. Raimondo* largely reversed its seminal decision in *Chevron v. Natural Resources Defense Council*—the 1984 precedent that called for judges to give deference to federal agencies' interpretation of laws passed by Congress. The ruling was also called the "Chevron deference" or "Chevron Doctrine." It played a massive role in the growth of the administrative state because it gave great weight to agency interpretations of ambiguous laws.

How Congress writes laws

To most people, federal laws mean Congress passes a specific law that the agencies enforce exactly as Congress specifies. In practice, however, Congress often passes a law that empowers an agency to create and enforce rules and regulations based on the principles of the law – the rules and regulations are not specified by Congress. This process exists because Congress lacks the expertise to write detailed laws for many highly technical subjects. A less-discussed aspect is that Congress delegates day-to-day implementation to the agencies, which have more expertise and time to create the details. The clear downside of this approach is that it transfers enormous power to the agencies.

The implications of Loper Bright

The Loper Bright decision effectively removes this deference unless Congress clearly delegates to the agency the ability to determine how an ambiguous law would be applied in practice. Today, in light of Loper Bright, a federal judge has the sole power to determine what an ambiguous law means and can take input from almost anywhere.

This is a significant shift of power from the executive to the judicial branch and raises issues about a judge's expertise to determine what Congress intended. How will the judge be educated, and how long will the process take?

Issues around forum shopping will come into play as interested parties try to steer cases to sympathetic judges. How many times will challenges be filed in the Northern District of Texas yet their appeals are heard by the U.S. Court of Appeals for the Fifth Circuit? This is going to get messy for a lot of agencies and the people and companies they regulate.

For example, IT and Security teams in finance have been preparing for the SEC to finalize new rules around Enhanced SCI. What happens if this work is put on hold for a legal challenge or a judge rules the proposed regulation is unconstitutional and stops the update? That means lots of wasted time and the process could repeat for years. Companies need clarity in what is expected from the law and a timeline for compliance.

A prediction

It seems likely that by late Q1 or Q2, 2025, an industry trade group will file suit to challenge key federal cybersecurity regulations. It may start with the SEC's proposed amendments to Regulation SCI. Cybersecurity regulations created under the umbrella of the Gramm-Leach-Bliey Act are at risk as well. Healthcare cybersecurity regulations tied to reimbursements under the authority of the Centers for Medicare and Medicaid Services (CMS) are another set of regulations that may be targeted.

A cautionary scenario

Suppose a federal judge grants an injunction that stops updates to Regulation SCI. The SEC's position is given minimal weight by the court, substituting its own expertise and judgment over the law and facts and overruling the SEC to strike down the proposed rule. After 3 to 5 years of appeals, the issue makes its way to SCOTUS, the judgment is affirmed and the proposed rule is dead.

On the other hand, perhaps Congress responds by passing clear laws that clearly describe the agency's role in interpreting statutes. In any event, life continues for IT and Security teams who are already overwhelmed and simply want a clear set of rules.

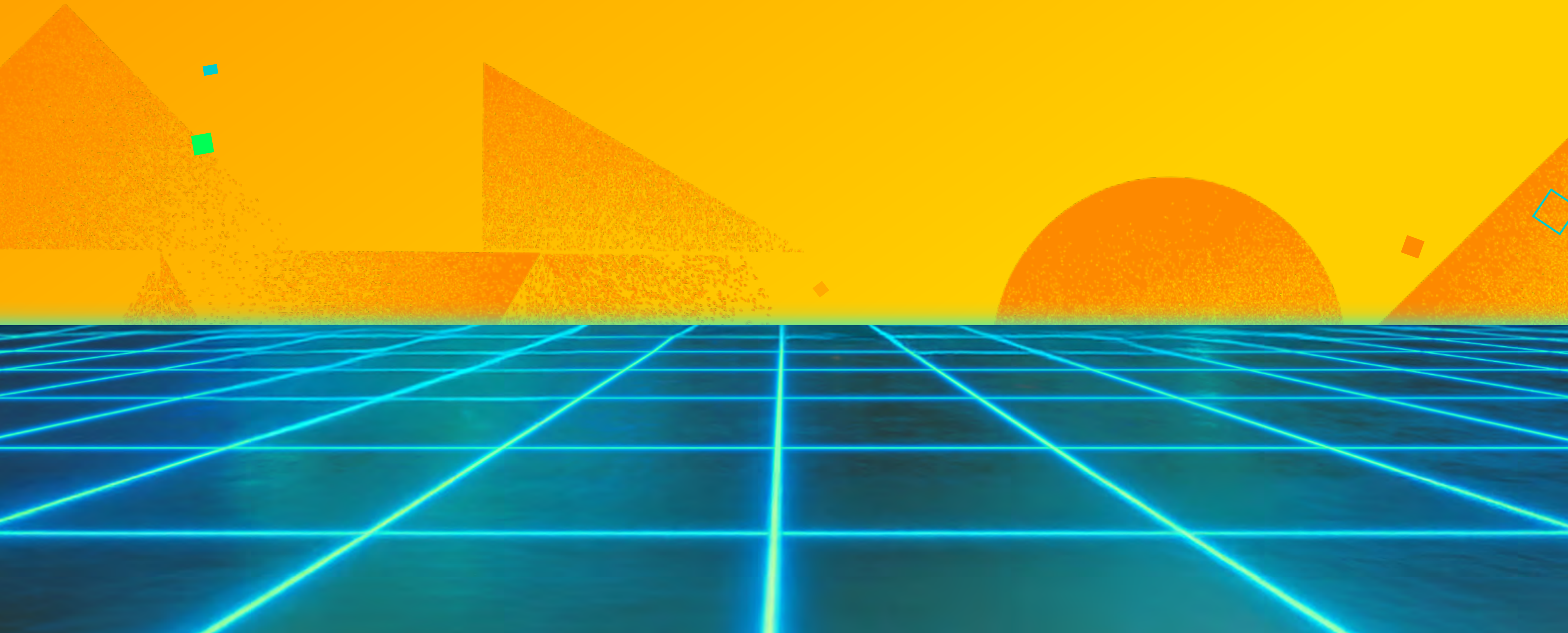
The road ahead

It will take time for Loper Bright's impact to work through the federal courts, agency rulemaking process, and Congress. The legal impact is mostly uncertain, but the practical impact is clear. IT, Security, and GRC teams will be in limbo because future regulation implementation is unclear, and several key cybersecurity regulations may soon be called into question.

What can IT and Security teams do? It is now more important than ever to make forward-looking architectural decisions that focus on agility and include flexible, open telemetry management frameworks so that regulatory changes become minor adjustments instead of significant, expensive re-engineering efforts. Otherwise, teams risk getting caught unprepared and must put aside business-critical work to re-engineer processes to comply with federal regulations.

Chart a path in a complex digital future

As we enter 2025, the path forward for IT, Security, and Compliance teams will demand adaptability, innovation, and a proactive approach to managing change. By understanding emerging trends and applying strategic insights, organizations can turn challenges into opportunities and position themselves for success in a dynamic digital and regulatory landscape. Whether it's navigating uncertain cybersecurity regulations, optimizing telemetry data management, or integrating AI responsibly, the decisions you make today will shape your resilience tomorrow. Let this eBook be your guide to help you navigate the complexities of the future with confidence and clarity.



Cribl®

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Powered by a data processing engine purpose-built for IT and Security, Cribl's product suite is a vendor-agnostic data management solution capable of collecting data from any source, processing billions of events per second, automatically routing data for optimized storage, and analyzing any data, at any time, in any location. With Cribl, IT and Security teams have the choice, control, and flexibility required to adapt to their ever-changing data needs. Cribl's offerings — Stream, Edge, Search, and Lake — are available either as discrete products or as a holistic solution.

Learn more: cribl.io | Try now: Cribl sandboxes
Join us: Slack community Follow us: LinkedIn and X (Twitter)