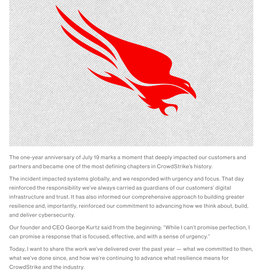
One Year Later: Reflecting on Building Resilience by Design

July 14, 2025 | Mike Sentonas | Executive Viewpoint



The one-year anniversary of July 19 marks a moment that deeply impacted our customers and partners and became one of the most defining chapters in CrowdStrike's history.

The incident impacted systems globally, and we responded with urgency and focus. That day reinforced the responsibility we've always carried as guardians of our customers' digital infrastructure and trust. It has also informed our comprehensive approach to building greater resilience and, importantly, reinforced our commitment to advancing how we think about, build, and deliver cybersecurity.

Our founder and CEO George Kurtz said from the beginning: "While I can't promise perfection, I can promise a response that is focused, effective, and with a sense of urgency."

Today, I want to share the work we've delivered over the past year — what we committed to then, what we've done since, and how we're continuing to advance what resilience means for CrowdStrike and the industry.

Strengthening Platform Resilience

Over the past year, we've focused deeply on advancing resilience across our platform and the company. This was never about quick fixes or surface-level improvements; it's about advancing the Resilient by Design principles George outlined at Fal.Con last year to drive greater resilience across our ecosystem.

We have long operated in and secured some of the most mission-critical environments in the world. That responsibility continues to shape how we design for performance, scale, and resilience.

Resilient by Design is anchored by three core pillars, shaping how we strengthen the platform, protect customers, and advance resilience at scale.

Guided by this approach, we've evaluated everything from how we build and test to how we operate and support our customers. What follows is a closer look at the work we've done and how these principles continue to guide our progress.

The Three Pillars of Resilient by Design

Foundational: Resilience is a foundational element of our company. Our customer-centric approach continues to enhance resilience, from code and deployments to configuration and support, strengthening every aspect of how we build and operate.

Adaptive: We continue to advance a platform that doesn't just react to problems but increasingly learns from operational data, anticipates potential issues, and evolves with automated safeguards designed to reduce recurrence. It's about creating intelligence that responds dynamically to changing conditions, diverse environments, and evolving threats.

Continuous: Our focus has been to continue driving an ongoing feedback loop that enables constant learning and adaptation. It's about building systems that strengthen themselves across interactions, deployments, and customer environments.

We outlined some immediate steps we took after the incident. But we didn't stop there. Over the past year, we've made additional lasting changes that drive proactive resilience.

The pillars of Resilient by Design guided our comprehensive improvements across several key areas:

1. Sensor and Content Safety

At the core of our drive for advancing resiliency is our **Sensor Self-Recovery** capability, which detects crash loops and automatically transitions systems into safe mode. Our Windows and macOS sensors intelligently recognize problematic states and self-correct without human intervention. We've also introduced the **Sensor System Remediation Toolkit** for out-of-band recovery, helping to ensure we can return systems to operational status.

In parallel, we implemented a new **Content Distribution System (CDS)**, which uses a new ring-based, automated deployment model, guided by golden signals. This extends the rigorous testing principles used for core software to every content release.

2. Setting New Standards for Customer Control

As part of our platform-wide improvements, we've reimagined how customers control updates and configurations, providing greater transparency, flexibility, and precision so customers can manage updates in a way that works for their unique environments.

Figure 1. Customers can control update timing and configuration with greater transparency, flexibility, and precision.

CrowdStrike's Falcon platform is a cloud-native, AI-powered platform that protects customers through a combination of on-device prevention engines and real-time intelligence from the CrowdStrike Security Cloud. Our detection capabilities are continuously enhanced via configuration updates, not definition files, delivered with precision and validated for accuracy.

Our customers have always had control over when and how their Falcon sensor versions are updated. But after July 19, we understood that customers wanted even more control over how and when security configuration updates are applied to their environments. What started as an immediate response to customer feedback has evolved into something more significant — a complete reimagining of the relationship between security vendors and their customers.

Beyond our internal improvements, we've made significant enhancements to how customers interact with and control our platform. Our new content control capabilities give customers greater flexibility in managing updates. Through host group policies, customers can set different deployment schedules for test systems, workstations, and mission-critical infrastructure.

Our content quality dashboard provides real-time visibility into how releases are progressing across early access and general availability phases. Customers can see exactly when individual hosts last received updates and use Falcon Fusion SOAR workflows to automatically adjust deployment settings based on their operational needs.

We've also introduced content pinning, which gives customers the option to lock their systems to specific content versions and offers precise control over when and how updates are applied. This provides additional flexibility for customers with unique operational requirements or strict change management policies.

We didn't just add a few content configuration options; we fundamentally rethought how customers could interact with and control enterprise security platforms, creating more granular controls and expanding the flexibility available to those who need it.

3. Infrastructure and Operational Excellence

Over the past year, we've expanded and strengthened the digital operations capabilities that have long supported our global infrastructure, which include real-time telemetry, system health monitoring, and incident management processes driven by our engineering and reliability teams.

To further scale and unify these efforts, we've established a new, purpose-built **Digital Operations Center**. This dedicated facility brings together those distributed capabilities into a single command center, giving us deeper visibility and faster response across millions of sensors worldwide. This reflects our ongoing investment in operational excellence and is designed to meet or exceed the standards of the world's leading technology operations centers.

In addition, our multi-cloud, hybrid cloud infrastructure delivers elastic scaling capabilities, ensuring we can respond to any demand scenario. Today, we operate at exabyte scale, processing telemetry from millions of systems — including endpoints, devices, clouds, containers, and more — while maintaining the performance and reliability our customers depend on.

4. Quality and Testing Innovation

With the introduction of the **Falcon Super Lab**, we've enhanced our already rigorous quality control processes, testing thousands of OS, kernel, hardware, and third-party application combinations and interactions. Building on this foundation, we will also be delivering customer profile testing, a methodology that allows us to validate our products as they're deployed in specific customer environments.

We have continued our partnership with outside leading experts to provide regular code reviews, which now span our code, quality processes, and operational procedures. These reviews, combined with ongoing internal improvements, have helped us continue to optimize platform performance, maintainability, and reliability across a broad range of environments.

In parallel, we've strengthened our enterprise resilience practices. Over the past year, we've increased the frequency and rigor of resilience exercises to ensure our teams, processes, and technology are prepared to operate under pressure and maintain continuity in a multitude of scenarios.

5. Operational Incident Management

We've strengthened how we manage technology incidents, building on a foundation of speed, discipline, and precision. Our sensor hardening initiatives proactively identify and prevent potential failures before they impact customers. Together, these enhancements help ensure our systems are better prepared for the unexpected and designed to operate under pressure, reinforcing our commitment to resilience at every level.

Our Ongoing Commitment

This work isn't finished and never will be. Resilience isn't a milestone — it's a discipline that requires continuous commitment and evolution.

To ensure that resilience remains central to everything we do, we will soon be bringing on board a new executive: **Chief Resilience Officer**. Reporting directly to the CEO, this person will help shape how we build, operate, and lead across engineering, operations, and the business. After an exhaustive search, we will announce this hire soon. We expect more companies will make moves like this in the future to ensure that business resilience is owned at the highest levels.

This commitment to resilience extends beyond our leadership structure. We've continued to strengthen our existing enterprise resilience practices, which encompass continuity planning not just for technology but for the people and processes that support our customers every day. Our multi-year approach has earned us ISO 22301 certification, the international standard for business continuity management systems, recognizing that our resilience program meets globally recognized standards.

In addition, our **collaboration with Microsoft** continues to drive progress for our industry. We recently announced a collaboration to bring clarity on how adversaries are identified and tracked across vendors for the benefit of all cybersecurity teams. And we continue to collaborate toward greater platform resiliency through our active engagement in the Windows Endpoint Security Platform (WESP) initiative. This builds on CrowdStrike's long history of aligning with Microsoft's certification and testing procedures.

The reality is that kernel-level access remains critical for comprehensive cybersecurity. Today's adversaries operate at the kernel level, exploiting the tens of thousands of legitimate drivers that run with kernel access. Security must meet the threat where it exists.

CrowdStrike made early architectural decisions to minimize kernel-invasive approaches wherever possible. And as Microsoft introduces new capabilities that allow for the development of security capabilities in user space that have parity with (or even surpass) kernel capabilities in efficacy, security, and performance, we will actively evaluate and adopt these features. But they cannot compromise security effectiveness.

To this end, we're launching **Project Ascent** under our newly formed **Chief Technology Innovation Officer** (CTIO) organization, led by Alex Ionescu. In close collaboration with our engineering department, this project will explore how we can uniquely leverage emerging platform capabilities, including those outside of kernel space, alongside new features introduced through Microsoft's WESP. While we continue working with Microsoft and adopt new capabilities as they mature, we'll continue to advance our own path, ensuring we can deliver greater resiliency, maintainability, and agility without compromising the visibility our customers seek from CrowdStrike.

Every day, our team is working on the next generation of resilience capabilities. We're not just building a more resilient CrowdStrike, we're working on approaches we believe will raise the bar for resilience across the cybersecurity industry.

Looking Forward

A year ago, we faced a moment that deeply impacted our customers and partners, one that pushed us to evolve how we think, build, and lead. Today, I'm confident we've emerged as a fundamentally stronger company with a platform and team that reflect the highest standards of resilience, built on the lessons of the past year and our commitment to continuous improvement.

The work continues, the commitment remains unwavering, and our customers can be confident that the platform protecting them today is stronger, more resilient, and more reliable than ever before.

To every customer, partner, and CrowdStriker — thank you for standing with us and standing for our mission: stopping breaches.

Related Content

How the CrowdStrike Falcon Platform Drove the Germany-Singapore Team to Success at NATO Locked Shields 2025

CrowdStrike and Microsoft Unite to Harmonize Cyber Threat Attribution

Announcing the CrowdStrike 2025 Global CrowdTour: Bringing the Power of the Crowd to a City Near You

« How the CrowdStrike Falcon Platform Drove the Germany-Singapore Team to Success at NATO Locked Shields 2025

CATEGORIES

CONNECT WITH US

FEATURED ARTICLES