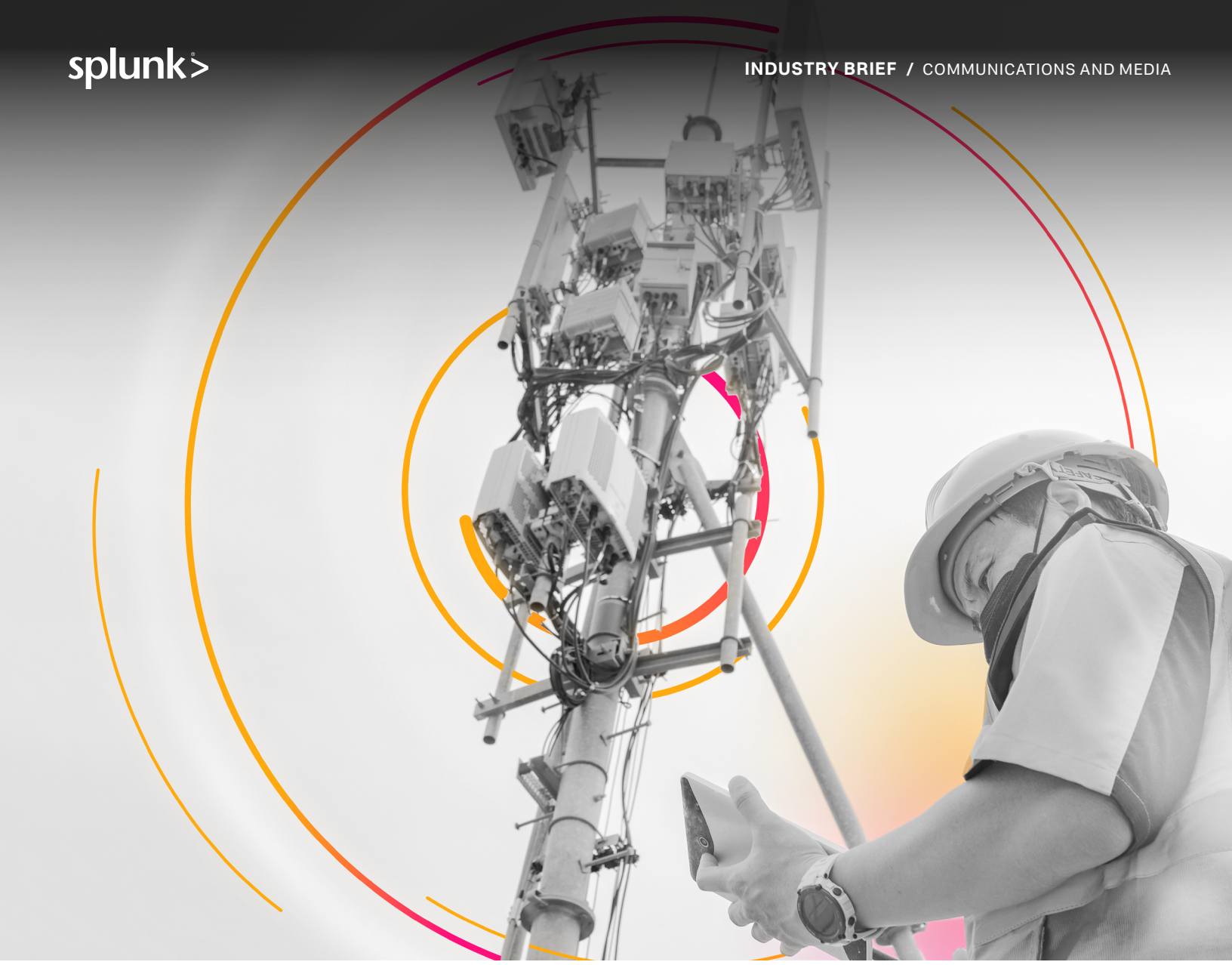


Protect the digital landscape with modernized security operations for Communications and Media

Today, we take for granted that we can interact with anyone, anywhere, whenever we want.

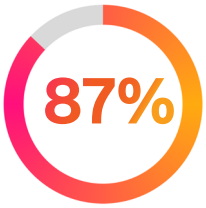
We have Communications and Media organizations to thank for this always-on connectivity. They provide the critical infrastructure that underpins our digital world, powering everything from banking to healthcare to transportation and more.

But as technology advances, and we rely more and more on communications networks, cyber threat actors are taking notice.

Hackers and state-sponsored agents are targeting telecom networks, either to steal sensitive customer data (including demographic and financial details), create widespread disruption — or both.

For example, some bad actors infiltrate communications and media systems to steal international mobile subscriber identity (IMSI) numbers or users' identifying information. Then, they can deploy systematic simjacking campaigns against dozens — or even hundreds — of victims.

What's more, Communications and Media organizations have faced:



of the largest distributed denial of service (DDoS) attacks.

increase in year-over-year double-extortion ransomware attacks.

And that's just the tip of the iceberg.

Communications and Media organizations are also responsible for securing hybrid environments that include both cloud and legacy infrastructure, millions of mobile phones, an expansive partner ecosystem and a growing number of IoT devices. And the rise of next-generation 5G and broadband services has only added complexity as organizations engage with a wide ecosystem of shared customer data and system interfaces.

Advancing digital resilience can help Communications and Media organizations remain trustworthy service providers and stewards of customers' sensitive information.

Building towards the SOC of the future is key to advancing digital resilience.

But it's hard to do this today.

Rapid technological change is expanding the attack surface. Fueled by digital transformation and industry consolidation, organizations' hybrid environments have expanded — with increased potential for points of failure due to cyber threats and system outages. With dynamic and sprawling networks, critical services and information are shifting further from the center, making it harder to manage and easier for disruptions to occur.

Siloed tools and teams are causing SecOps chaos. As Communications and Media organizations grow, particularly through M&A, they're acquiring various tools and teams that don't always integrate and collaborate with one another. Many business units are duplicating efforts, and it's hard to know who is doing what to effectively detect, investigate and respond.

Limited innovation capacity is increasing risk. It can be costly to maintain multiple tools and solve for disruptions, leaving less money to invest in new innovations that drive the organization forward. And innovating can be a challenge with inflexible tool sets that lack customization capabilities.

79% of security leaders think a loss of productivity will put them at risk of being out-innovated.

But with a better view of networks and the customer journey, innovation won't have to stop at what we can imagine today. Communications and Media organizations will have the insight they need to continue to improve their offerings and find new ones.

Digital resilience is a catalyst to driving security operations center (SOC) enhancements that address these challenges head on. Organizations are building towards the SOC of the future, where unified threat detection, investigation and response drive critical outcomes:

- Mitigating the impact of security incidents
- Improving readiness for regulatory imperatives
- Decreasing the impact of previous attacks
- Shifting to more proactive security
- Securing digital transformation efforts

The more the digital landscape expands, the more important security will be

Given the growing attack surface, visibility is the first step toward building the SOC of the future. Gaining a full view of everything from legacy (and often siloed) infrastructure to cloud-based architecture and software-defined networks in one place is essential, so organizations can pinpoint exactly where threats are happening and ix any issues before significant problems occur.

This unified view of the digital landscape keeps telecom networks operational and secure. It's a foundation not just for secure operations, but for the future of their business. By demonstrating how they can modernize their security posture to protect critical infrastructure, organizations can build trust and credibility in next-gen services.

Next-gen services are a global call to action for improved security

Communications and Media organizations are looking for digitally resilient systems to safeguard their networks and provide essential infrastructure for critical industries — and Splunk helps do just that. Splunk provides full visibility across the digital landscape to maintain a secure environment for customers, employees and digital suppliers.

With Splunk, organizations can:

Reduce business risk
Achieve comprehensive visibility and detection to detect threats faster, gain context rapidly and address risk proactively.

Protect against sophisticated threats
Proactively monitor for threats using machine learning-powered threat detection, and prioritize those that compromise the business and personally identifiable information (PII).

Power a SOC of the future
Unify threat detection, investigation and response to automate SOC processes and meet compliance requirements.

Detect fraud
Isolate indicators of subscriber fraud and automate alert actions to block fraudulent activity.

Fuel security innovation
Engage with the vibrant Splunk Community to find answers to challenges and access partners, applications and threat research.

Investigate and respond rapidly
Investigate anomalous activity and enrich, contextualize and prioritize high-fidelity alerts to shorten triage times and raise true positive rates.

Splunk empowers the entire security journey

Digital resilience is a journey. But the path is far from linear — and, it can vary greatly. So, Splunk has created a model to help security teams expand into new and complementary use cases that advance security operations. It takes organizations from getting visibility to being more prioritized and proactive, integrating workflows in and between teams for safer and more resilient digital infrastructures.

Powering the SOC of the future

journey stages

Foundational Visibility

See across environments

Search, monitor and investigate for real-time security monitoring

Attain a consolidated view of aggregated logs from all digital touchpoints to improve threat detection, incident investigation and response.

Guided Insights

Detect threats and issues with context

Reduce noise, detect more threats and identify risk with AI/ML-powered detections

Detect threats proactively across legacy systems and cloud-native applications using an AI/ML-powered, risk-based approach and comprehensive threat intelligence to stop advanced attacks and slash dwell time.

Proactive Response

Get ahead of issues

Accelerate incident investigations and response using automation

Embrace automation across threat analysis, containment, response and recovery actions increasing your security team's productivity and efficiency while ensuring the reliability of customer-facing applications.

Unified Workflows

Collaborate seamlessly

Maximize SOC efficiency with integrated threat detection, investigation and response

Deliver a great customer experience by monitoring the entire user journey supported by unified threat detection, investigation and response to strengthen digital resilience.

Forging ahead on the security journey with Splunk

Communications and Media organizations can strengthen digital resilience by building a SOC of the future with unified threat detection, investigation and response from Splunk Security.

As the industry leader in security operations solutions, Splunk is the foundation of the SOC of the future — providing an unmatched breadth of technologies, community and expertise. Splunk allows organizations to detect threats accurately, rapidly gain security and IT context for holistic investigation, and automate response to address risk proactively.

With increasingly resilient digital systems, Communications and Media organizations can prevent major issues that threaten the security and reliability of their digital infrastructure and quickly remediate issues that do occur — helping them focus on innovations that strengthen their business and keep customers happy.

Splunk customer benefits

90%

Faster at identifying the root cause of threats and determining appropriate remediation

50%

Increase in alert fidelity

30%

Increase in operational efficiency

Source: ESG Economic Validation Report, 2023

Learn more industry insights >

Learn more about security >