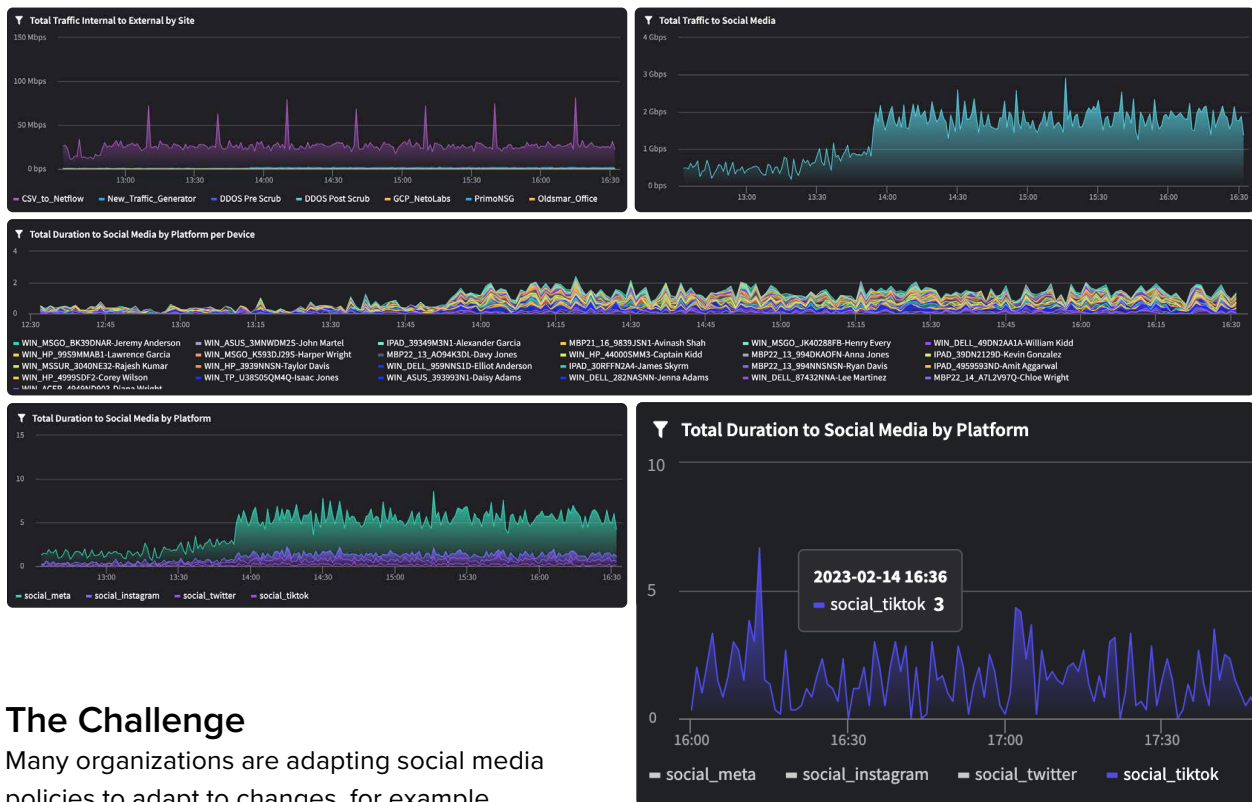


Solution Brief

Achieve Operational Governance of Social Media with Netography Fusion®

What is Operational Governance?

The mechanisms implemented by an organization to automate a continuous approach to testing the efficacy of an organization’s security controls against cyber threats and organizational policy.



The Challenge

Many organizations are adapting social media policies to adapt to changes, for example, blocking TikTok or protecting employees from misinformation or emotional stress. Yet, users are continuously accessing banned networks on endpoints. Moreover, at many organizations, it takes months to detect or report social media usage. For example, how do you know if your current social media firewall rules or endpoint detection and response (EDR) filters are working, being updated, or even configured properly? With Netography Fusion’s Operational Governance capabilities dashboards, you’ll get a real-time comprehensive view of all social media traffic.

Is your team currently supporting the organization by providing visibility and validation that social media policies are being followed? Are you able to answer yes to all of these questions?

Social Media Usage Control Effectiveness Validations:

- Are you able to detect if the social media policy controls and content filters are working? For example, are social media usage exclusions effective for employees vs. contractors or departments that have exclusions, e.g. is TikTok usage prohibited or permitted by specific users?
- Are you able to detect if an application's virtual machine is inappropriately connecting to social media networks?

Social Media Usage & Network Traffic:

- Are you able to provide details on social media usage by bandwidth consumed by location, department, role, or device?
- Are you able to provide details on social media usage by time of day?

Social Media Usage & Operational Governance Controls for Compliance:

- Are you able to provide sufficient evidence when under audit or upon request that your organization has the verified controls to meet regulatory requirements? The FTC, FINRA, SEC, HIPAA, federal, state, and local governments, and other regulatory groups have strict rules for the use of social media, mostly centered on privacy, confidentiality & data security.

Operational Governance and Social Media

Organizations have numerous solutions available to them to block or monitor social media usage, including browser plugins, EDR and endpoint content filtering software, firewall configurations, and more. However, the increasing knowledge and sophistication of users enable some users in organizations to bypass these controls. Additionally, cyber threat actors have methods to compromise the known controls and in other cases, will use a vulnerability or other weakness to access social media on devices without controls.

Operational governance is particularly challenging for modern organizations with Atomized Networks, meaning they are dispersed, ephemeral, encrypted, and diverse. Security and network teams struggle to get scalable, continuous network visibility across the Atomized Network – legacy, on-premises, hybrid, multi-cloud, and edge environments. The pervasive use of encryption and unauthorized VPNs is blinding traditional network detection and response (NDR) tools that rely on deep packet inspection (DPI), and often each legacy or cloud environment has its own set of tools for monitoring and security with little overlap. This is where Netography Fusion takes the lead.



How Netography Fusion meets the challenges of Operational Governance for Social Media

Netography's SaaS-based architecture enables a rapid and low-friction deployment to deliver real-time visibility, detection, and response capabilities when and where they are needed across the entire Atomized Network.

We achieve this by ingesting flow logs from all of the major cloud providers – Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud, and Oracle Cloud – as well as on-premises infrastructure to drive a consistent and simple search language we call Netography Query Language (NQL). We offer API integrations that synchronize context labels, tags and alerts with an organization's EDR, cloud, security information and event management (SIEM), security orchestration automation and response (SOAR), and configuration management database (CMDB) platforms. This enables us to enrich flow logs with context in real-time at the time of ingestion.

Netography Fusion provides a single pane of glass and intuitive UI, so users have an easy way to get the answers they need about social media traffic—what's on their network, what it is doing, and what's happening to it.

Operational governance for social media is easy to implement with Netography Fusion and its included preconfigured dashboards, and the ability to create your own dashboards that align with your organization's social media usage policies. This can include:

Event alerting for social media network traffic that is a violation of policy. For example, you can set an alert that is sent to an email address, messaging platform or your SIEM.

Evidence for audits. For example, you can provide auditors with screenshots and detection models that demonstrate your ability to implement and verify organizational governance for social media usage.

Squash silos and build trust between teams. Support the teams from across your organization that are responsible for training, implementing, enforcing, and reporting on social media usage. Netography Fusion users can provide visibility on social media usage to authorized teams from the security operations center (SOC) to IT to Human Resources to Risk and Compliance.

Refine Your Operational Governance Program for Social Media

Netography Fusion's operational governance capabilities enable faster validation of new social media governance policy changes. With it, organizations can greatly reduce cyber threat risks and ensure that organizational policies and changes to them can be rapidly enforced and monitored in real-time.



About Netography

Netography® has created the first network-centric platform that reconstitutes capabilities disrupted by the combined impact of encryption and Atomized Networks across the security world. Netography Fusion® is for enterprise security operations center (SOC) and cloud operations teams that need scalable, continuous network visibility across the Atomized Network – legacy, on-premises, hybrid, multi-cloud, and edge environments.

Learn more at netography.com.