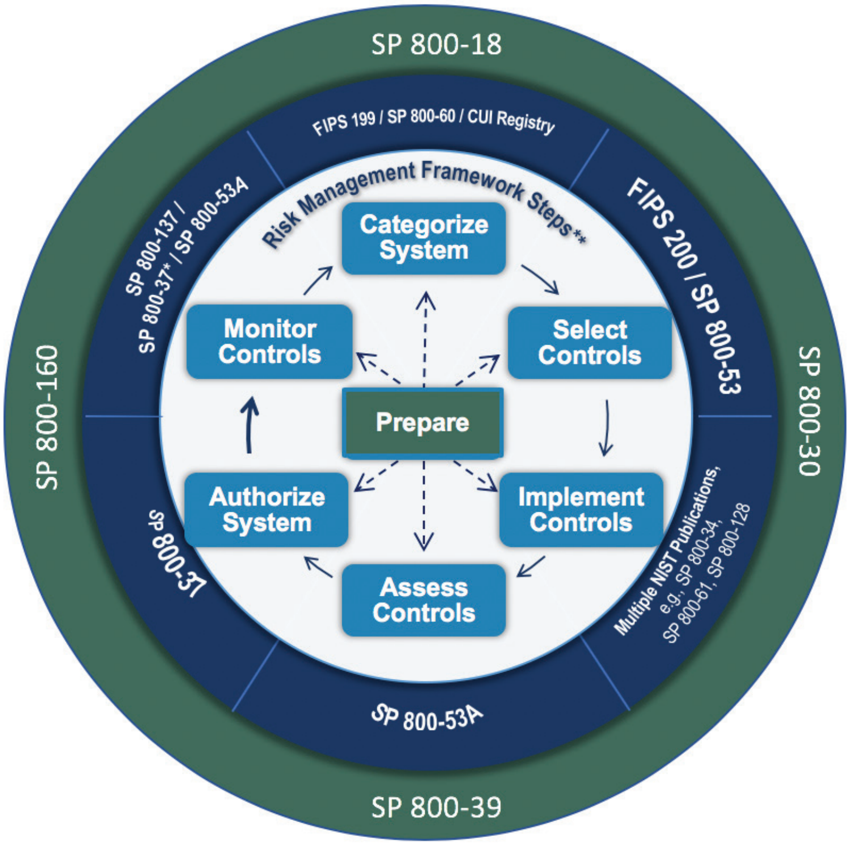
Xacta: The enterprise solution for cyber risk management and compliance automation.

The Xacta® suite of enterprise cyber risk management and compliance automation solutions helps you meet the complex challenges of managing IT risk with continuous compliance monitoring, security assessment, and ongoing authorization.

Optimized for the cloud and deployed at some of the world's most security-conscious organizations, Xacta enables you to fully automate the NIST Risk Management Framework (RMF) through automated workflows and automated document generation to produce the body of evidence (BOE) for Authorizing Officials (AO) and other risk executives to make educated risk decisions.

The core functionality of Xacta is geared to automate the security authorization process through the following key features:

- Automated categorization
- Push-button regulation transition
- Robust, multiple, and automatic inheritance
- Overlays and conflict resolution
- Document generation
- Workflow and actions / approvals
- Reporting / status visibility
- Automatically connect vulnerabilities to related controls
- Automated notifications
- Automated testing
- System of systems
- Cloud support and automation
- Questionnaire-based workflows



Source: National Institute of Standards and Technology (NIST)

Xacta streamlines and automates the NIST Risk Management Framework (RMF):

- **Xacta 360** supports system assessment and authorization across the enterprise, on-premises, in the cloud, and in hybrid environments.
- **Xacta.io™** enables continuous compliance of automated controls across multiple systems and standards.
- **Xacta Compliance Campaign Manager** streamlines compliance of manual controls through qualitative surveys and questionnaires.

Xacta: Manage IT risk with compliance automation, continuous monitoring and ongoing authorization.

The Xacta suite includes these solutions that work together to automate and streamline the NIST Risk Management Framework:

Xacta 360 streamlines and automates the NIST RMF and the associated assessment and authorization processes required for ATO. Xacta 360 analyzes IT asset information collected seamlessly from a variety of systems including workloads based in the cloud. It identifies, tracks, tests, and helps remediate security risks from the system up to the enterprise, and continuously monitors and audits compliance with the appropriate standards. And, it provides document generation and management, role-based access control, and a body of evidence (BoE) repository. Xacta 360 increases security authorization productivity through organizational improvements in effectiveness and efficiency. Standardization and organizational transparency are fundamental to Xacta. It's the solution of choice for managing complex cyber risk environments and compliance processes in the cloud, on-premises, and in hybrid environments.

Xacta.io enables continuous compliance of automated controls across multiple systems and standards. It correlates results from multiple security products across an organization into a single view and maps them to the relevant controls for security and risk management. Xacta.io ingests results from third party scanner tools in the enterprise to quickly analyze the relevant security controls. Xacta 360 then uses this analysis to address the continuous monitoring control requirements to keep the applicable authorization boundary within compliance. This enables automated security monitoring on standardized schedules according to the processes, procedures, and toolsets specified in the monitoring strategy. Xacta.io will provide trend analysis reporting of findings as well as develop mitigation plans for new and existing security control results as required.

Xacta Compliance Campaign Manager streamlines compliance of manual controls through qualitative surveys and questionnaires. Xacta CCM enables users to create and distribute OCIL-based surveys and questionnaires for manual security checks, enforce controls for government and commercial standards, and crosswalk controls from different frameworks for greater efficiency and less redundancy. This tool helps "automate" the non-technical, non-automatable controls by establishing campaigns to cover specific compliance objectives. Responses during these campaigns feed into Xacta 360 to validate tests during a risk assessment. All of these deployed tools are SCAP-compliant to produce and ingest data in this standardized format. This includes incorporation of all the SCAP elements, e.g., CVE, CCE, CPE, XCCDF, CVS, and OVAL). The tool suite also integrates OCIL requirements.

Contact Us for More Information

Xacta automates critical steps in NIST compliance processes and gives you the insights you need to manage risk in your cyber environment. Contact us today to learn how Xacta helps you take control of managing your IT security posture.

Telos®

info@telos.com | 800.70.TELOS (800.708.3567)
www.telos.com | twitter.com/telosnews
facebook.com/teloscorporation
linkedin.com/company/telos-corporation

Xacta-062020

Telos®

TELOS GHOST®

You can't exploit what you can't see.

- Be totally hidden and anonymous on the public internet
- Protect sensitive transactions with anonymous network access
- Work confidently with hidden mobile comms, email, storage, applications
- Cloud-based network-as-a-service; no hardware or software to buy or maintain

Many businesses and government agencies depend on extreme security and confidentiality in their operations. But they're at risk of their vital information being compromised when personnel need to connect with each other and with digital resources on the enterprise network or in the cloud.

At the same time, cyber protection and threat intelligence teams need to work undercover as they observe and study suspicious traffic, events, and actors in order to better defend their networks. Any leak of digital exhaust would be a disaster that could blow their cover, jeopardizing their mission, their organization, and perhaps their lives.

Telos Ghost®: Network obfuscation and managed attribution as a service for the ultimate in cybersecurity and secure operations.

The best way to protect people, assets, and information on the network is to prevent them from being seen in the first place. Telos Ghost is a virtual obfuscation network that provides privacy and security for worldwide communications and transactions over the internet through obfuscation, dynamic IP routing, and managed attribution.

You already use security solutions like VPNs and endpoint protection as well as secure network strategies such as zero trust network access (ZTNA), secure access service edge (SASE), and others. Telos Ghost complements and enhances those capabilities for applications where you absolutely *cannot* afford to take chances.

Telos Ghost:

- ✓ Obscures and varies network pathways to prevent adversaries from tracking users and information
- ✓ Uses multiple layers of encryption to protect information and remove source and destination IP addresses, eliminating network paths back to the source
- ✓ Enables users to manage their technical and non-technical persona to disguise their identity and location
- ✓ Hides critical network resources using cloaked capabilities for email, storage, applications and unified communications

Best of all, you are in complete control of the network. Offered as a shared or dedicated network-as-a-service, Telos Ghost allows you to own your own private network without the cost of designing, implementing, and managing it yourself.

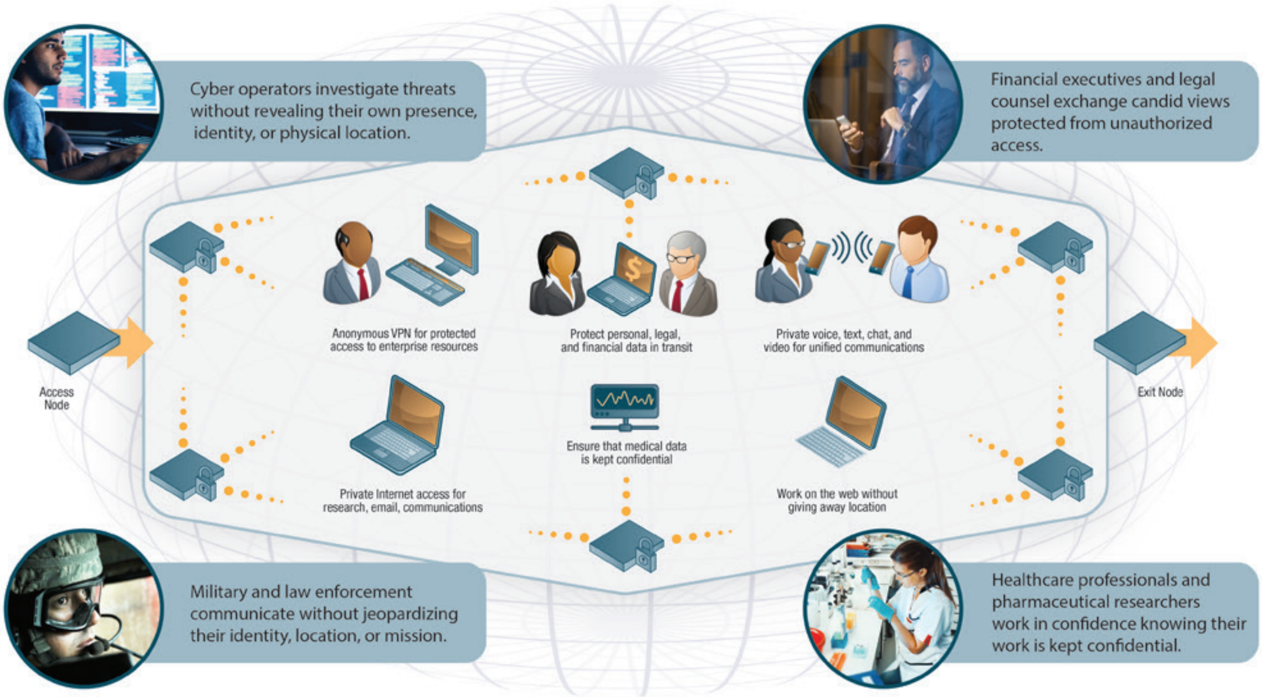
You can spin up a network for a temporary mission and tear it down in an instant. You can establish a permanent "private internet" for enterprise networking with greater security than leased lines, MPLS, and SD-WANs. All without revealing the existence of the network itself or giving away the presence, activities, and identities of your users.

Telos Ghost provides three essential and complementary capabilities for security and privacy:

Private Web Access: Secure anonymous internet access; disguises the identity and location of personnel when using the public web for cyber threat intelligence and competitive research.

Private Network Access: Leased-line security with VPN flexibility; allows authorized users to work with mission-critical enterprise information without being seen or discovered.

Cloaked Services: Hidden mobile communications, storage, and servers; enable users to securely talk, text, email, store information, and use video and applications over any mobile device


Anonymous VPN for protected access to enterprise resources
Protect personal, legal, and financial data in transit
Private voice, text, chat, and video for unified communications
Access Node
Exit Node
Ensure that medical data is kept confidential
Private Internet access for research, email, communications
Work on the web without giving away location

Cyber operators investigate threats without revealing their own presence, identity, or physical location.

Financial executives and legal counsel exchange candid views protected from unauthorized access.

Military and law enforcement communicate without jeopardizing their identity, location, or mission.

Healthcare professionals and pharmaceutical researchers work in confidence knowing their work is kept confidential.

Telos Ghost: the Measure of Security You Need for Mission-critical Requirements.

Telos Ghost protects personnel, information, and network resources in industries and applications where security and confidentiality are paramount:

Cyber Threat Intelligence – Keep threat intelligence researchers, cyber protection teams, and the evidence they collect hidden and anonymous

Military – Camouflage data and warfighters in garrison and in deployed locations; deliver network defense-in-depth across the DoD enterprise

Government – Protect senior leadership in remote/TDY locations; secure tax and revenue records, personnel files and transactions, other sensitive applications

Remote Workforce – Give deployed and work-from-home personnel a private internet that's unseen to the outside world for assured security and privacy

Law Enforcement – Disguise identities in undercover operations and cybercrime investigations; protect criminal justice records

Emergency Services – Hide sensitive information used by first responders, fire fighters, and search and rescue teams in disaster response planning and operations

Finance, Banking and Investments – Hide financial transactions and data sent between customers and investment firms, transfer agents, and securities markets

Healthcare – Ensure security and privacy of electronic health records; telemedicine exams; exchange of patient data between clinics and primary care facilities

Supply Chain Security – Make the critical elements of your supply chain invisible by obfuscating and encrypting transactions, storage, and servers

Critical Infrastructure – Conceal SCADA and ICS systems to protect diagnostics and maintenance transmissions; protect defense contractor data in a privatized network

Utilities – Securely monitor water treatment and distribution systems, power transmission, oil and gas infrastructure, HVAC systems

Telos Ghost: Protecting users and information across the network.

Security-conscious enterprises in business and government need a secure cloud network solution that provides high levels of obfuscation and encryption to protect their personnel and their information wherever their missions take them.

The unique architecture and capabilities of the Telos Ghost network provide high levels of security through encryption and proprietary-based mesh algorithms for dynamic IP routing among cloud transit nodes. The technology built into the Telos Ghost network provides a second level of security by providing complete anonymity of your users and their locations.

Learn more at www.telos.com/telos-ghost

Telos®

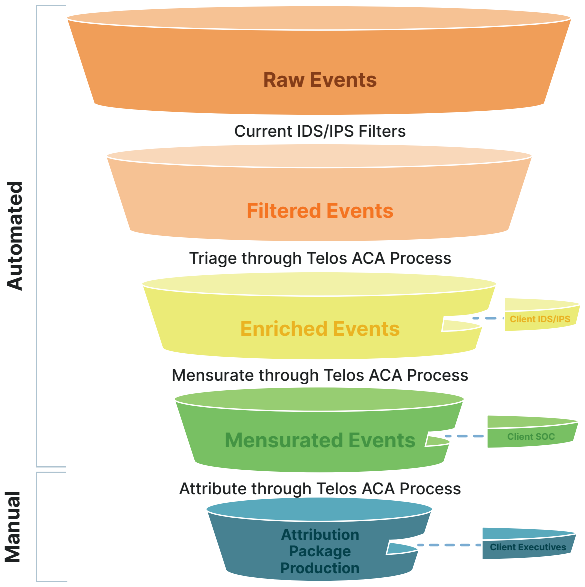
Telos Advanced Cyber Analytics

Telos® Corporation offers technology solutions and services that empower and protect the world's most security-conscious enterprises. We empower our customers with security solutions that leverage cloud technology, real-time collaboration, and mobile communications. We protect vital assets that include the critical operational and tactical systems of our customers so they can safely conduct their global missions. We serve the United States military, intelligence and federal civilian agencies, allied nations around the world, and members of the Fortune 500.

Common Issues In Today's Cybersecurity

Current cyber defenses struggle to keep up with the ever-changing and evolving adversary ecosystem. Lagging or out-of-date threat indicators and feeds further hamper organizations' ability to keep pace with the ever-evolving threat.

Many enterprises maintain a multitude of security tools, which exacerbates the issue of alert fatigue, and the added business costs of taking resources away from high-value tasks.



- Tailored Attribution Packages by customer request.
- Enriched data to provide absolute insight into IP addresses from a behavioral perspective.
- Insight into historical, positively identified activity on malicious and benign addresses.
- Ability to identify threat Origin, Infrastructure, Persona, History, and 60+ additional attributes.

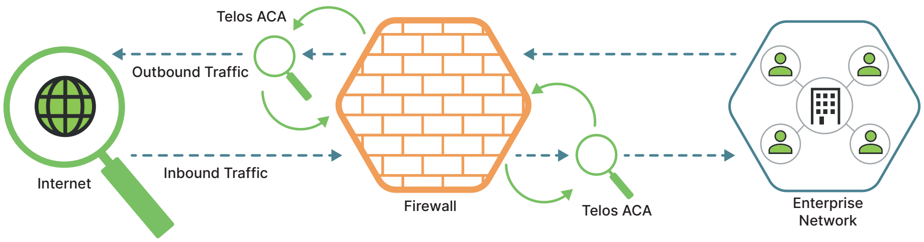
Triage consists of the automated enrichment of the data allowed to pass through the current IDS/IPS security protocols.

Mensuration consists of the automated illumination of the data to allow the SOC analysts to have an insight into the malicious intent associated with each triaged event.

Attribution consists of the manual compilation of the disparate data sets into a cohesive and intelligence package for consumption.

Telos Advanced Cyber Analytics

Telos Advanced Cyber Analytics provides actionable intelligence at speed and scale to the customer. The products provided are real- and near-real-time intelligence feeds and customized summary reports. The Telos solution enriches data that an organization assesses as low risk and applies sophisticated cybersecurity and intelligence methods beginning with two starting points: internal information provided by the customer and external information and intelligence obtained globally and correlated against the context of the client's operating environment. With machine learning to automate external data collection and assessment, Telos ACA determines patterns of behavior exhibited by threat actors, and provides the necessary information to reduce vulnerabilities within the IT infrastructure before attackers can exploit them.



The Telos ACA offering allows your organization to reduce the barriers in adopting advanced analytic technologies through a reduction in the need for complicated infrastructure, in-house subject matter experts, and the ongoing support costs of locally managed systems.