World Wide Technology

Unified Cyber Platform (UCP)

Sense, Identify, Collect, Alert, Act

A portable, scalable, coordinated Cyber Defense sensor data collection and processing framework for today's modern Federal security requirements.

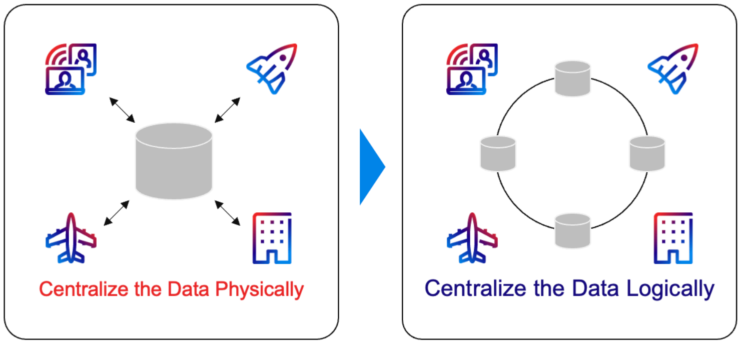
The problem

Government security teams are overwhelmed. Perpetually growing networks leading to increased attack surfaces, combined with unrelenting threat actors assaulting thinly stretched, low density / high value cyber talent professionals make it difficult for government security teams to simply maintain security operations, let alone stay ahead of attacks. Adding to the complexity are environments with disparate technologies and solutions that each solve a unique problem but are extremely difficult to unify. In addition, E.O. 14028 aims to increase the Federal Government's visibility into threats, ultimately requiring a data architecture that can support data collection and sharing at scale.

The solution

The key to effective cybersecurity lies in identifying malicious activity across government networks. Traditional log management and packet capture solutions promise much, but they don't provide the scalable and modular capabilities necessary to holistically and effectively capture and analyze traffic in today's ever expanding, disparate, cloud-based networks, especially data at the edge.

WWT's Unified Cyber Platform (UCP) delivers an innovative, scalable, portable, yet flexible solution that integrates several leading best-of-breed technologies to collect and analyze log data from across the network and combine it with Security Orchestration and Response (SOAR) automation to more effectively identify and mitigate cybersecurity threats. With UCP, customers can easily integrate a variety of technologies without disrupting existing infrastructure and have a single source of intelligence regarding security threats on the network at any location – physical, virtual or cloud.



Why WWT

WWT designs, builds, demonstrates, and deploys innovative technology products, integrated architectural solutions, and transformational digital experiences for customers around the globe. This is done through a collaborative ecosystem consisting of thousands of IT engineers, hundreds of application developers and unmatched labs for testing and deploying technology at scale.

WWT has long-term strategic relationships with the world's leading technology OEMs, including Cisco, Dell Technologies, F5, HPE, Intel, Microsoft, NetApp, Palo Alto Networks, VMware, Axellio, Redhat and Elastic. This provides direct access to millions of products from thousands of vendors & global distributors. This ability to integrate technology from multiple OEMs leads to game-changing tailored, holistic solutions.

To learn more, visit us at wwt.com.

The technology

The key to effective cybersecurity lies in identifying malicious activity across government networks. Traditional log management and packet capture solutions promise much, but they don't provide the scalable and modular capabilities necessary to holistically and effectively capture and analyze traffic in today's ever expanding, disparate, cloud-based networks, especially data at the edge.

Customers require solutions that adapt & pace evolutionary threats presented by learning adversaries. UCP is purpose-built to adapt and integrate evolving software applications and capabilities as required using RedHat OpenShift to enable evolution with evolving Cyber Technology.

Key features

A single, scalable solution based on commodity hardware that is small enough to be transported in a commercial aircraft as checked baggage and can scale to multi rack data center configurations. With UCP's integration capabilities, additional capacity can be added to expand the compute and storage of the system, with simplicity. With UCP, users can simplify operations, training and maintenance requirements.

High Speed Packet Capture (PCAP) powered by Axellio PacketXpress®. PCAP based analysis is a key capability to meet the requirements of cyber-security & protection from advanced persistent threats and nation state adversaries. Collection and Analysis at the packet level affords exceptional threat identification rates and "best in class" opportunity to coordinate analysis and damage assessment. UCP writes PCAP formatted files to filesystem at up to line rate (10Gb, 40Gb, 100Gb) sustained without packet loss.

DevSecOps ready capabilities: UCP comprises a modular, microservices-based architecture that communicates using open, RESTful APIs, which enable it to be configured for interoperability with other UCPs and other data processing and storage infrastructures. Additionally, UCP enables enterprise and tactical cyber systems to take advantage of benefits of containerization. Container platforms are quite common in data centers but slow adoption at the edge hinders alignment with the "agile vision."

Simple operations – connected or disconnected: UCP is automated and deploys RedHat OpenShift on bare metal, eliminating the virtualization layer completely – one less thing to learn and maintain. VM's and applications that are not container native are placed inside of containers using OpenShift virtualization, enabling tactical operators to support container native deployments and eliminate the burden of maintaining a virtualization layer concurrent with a container management system. UCP system operations are the same regardless of the operating environment or the deployment model; disparate configurations and baselines are eliminated; and the same management tools are used across configurations.

How

Multi-site and disconnected operations: WWT understands the challenges of working in degraded and disconnected environments and has a long history of supporting the Department of Defense. UCP has successfully demonstrated the ability to operate fully-stand alone in a disconnected environment in support of ongoing Cyber Operations. When UCP connects to the network, it can share data with other systems and analysts at remote locations can login / operate the system side-by-side. Consistency and management across deployed UCP systems is provided through RedHat Advanced Cluster Management for Kubernetes while controlling clusters and applications from a single console, with built-in security policies. Applications are deployed, policies enforced, and multiple clusters are managed at scale throughout the entire organization.