Securing and Automating Networks for the Oil and Gas Industry

Digital transformation is a key enabler in the oil and gas industry to reduce costs, make faster and better decisions, and increase workforce productivity. With current pricing pressure, global instability and increased emphasis on climate change, oil and gas companies are continuing to adopt digital technologies to increase efficiency through big data, analytics and sensors as well as to automate highly sensitive tasks. This adoption is critical in enabling oil and gas companies to achieve greater operational excellence – critical in today's turbulent environment.

On the downside, digitization is ramping up the stakes for cybersecurity. In a 2019 survey of oil and gas executives, a whopping 60% had a recent significant cyber-attack. Therefore, as oil and gas companies pursue digital transformation and related IT and OT convergence initiatives, the challenge is how to do this without impacting the critical sensors and control networks that must remain operational 100% of the time.

An often-underestimated component of a company's digital transformation efforts is the network infrastructure. According to the Gartner report **"Make Networking a Critical Strategic Infrastructure Resource for Enabling Digital Business"**, digital business initiatives will struggle unless organizations change the way they think about networking. Traditional network offerings are not well-suited for rapid delivery of new services, real-time responsiveness to the business and delivering massive scalability. Gartner's recommendation is to enable greater network agility by increasing network simplicity and automation.

Extreme, a leader in end-to-end cloud-driven networking solutions, offers a compelling solution to oil and gas companies looking for a simpler and more agile network that also offers improved resiliency and security. Through a combination of our innovative Fabric Connect networking technology, a comprehensive Wi-Fi portfolio, network access control, IoT security as well as intelligent AI-driven cloud-based management, oil and gas companies can transform their operations and embrace the digital technology they require, while protecting their critical infrastructure and control systems from the threat of a catastrophic cyber-attack.

Specifically, Extreme can offer oil and gas companies:

- Simple, streamlined automated network to increase efficiency and reduce costs
- An inherently secure network that is easily segmented into secure zones providing increased protection for Industrial Control Systems and other mission critical services

- Secure on-boarding of IoT/ IIoT devices with efficient processing of IoT/IIoT data at the edge
- High performance and highly reliable multicast for video surveillance and some PLC topologies
- High performance Wi-Fi for indoor, outdoor and hardened environments
- End-to-end AI-driven cloud management for network automation, assurance and insights
- Broad eco-system that consists of Industrial Ethernet vendors, video surveillance vendors, hypervisor vendors and security vendors

Simple, Automated Network to Increase Efficiency and Reduce Costs

The foundation of Extreme Network's Secure Automated Network Architecture for the Oil and Gas industry is an innovative networking technology called Fabric Connect. Fabric Connect (based on industry standard IEEE/IETF Shortest Path Bridging) was designed to make networks more flexible, more resilient and more secure. It eliminates the need for complex protocol overlays and eliminates touch points, making extending network connectivity and conducting moves, adds and changes, faster and easier.

It is a next generation network virtualization technology that abstracts network services from the underlying physical infrastructure, making it far easier to enable services where ever and whenever needed. Based on an Ethernet forwarding construct, it uses IS-IS routing as the control plane. It was designed to preserve the plug and play benefits of Ethernet while eliminating the challenging parts; flooding and learning, VLAN and MAC address scaling limitations and the need to block ports.

What makes the technology unique is its ability to support any network service (Layer 2, Layer 3 VRFs, unicast and multicast as well as IPv4 and IPv6 routing) and extend those services anywhere that is required with just a single control plane and edge only provisioning. Being standardized by both the IEEE and IETF, Fabric Connect is fully compatible with today's routers and switches, enabling both traditional networking as well as virtualized networking simultaneously, enabling companies to transition to virtualized networking at their own pace.

Fabric Connect is uniquely designed to deliver on the Oil and Gas industry's quest for operational excellence, having been field proven to reduce operations costs by as much as 66% while at the same time increase time to service by 11x.

Another major benefit of the Fabric Connect technology is its dynamic auto-attach capabilities. Auto-Attach (IEEE draft P802.1Qcj) provides for automatic attachment of users, devices, and virtual machines (VMs) to connect to Fabric Connect-based services. It uses extensions to the IEEE802.1AB Link Layer Discovery Protocol (LLDP) to automatically attach network devices to the right fabric service quickly and efficiently. When the end point disconnects, the service is retracted with residual configuration dynamically removed from the edge switch. This auto-attach capability can be deployed on endpoints, such as IP surveillance cameras, wireless APs, hypervisors (ESX-, HyperV- and KVM-based environments) and/or Industrial Ethernet access layer switches (for example Microsens and Belden-Hirschmann switches) so that seamless communication with the Fabric Connect network is possible throughout the eco-system.

Fabric Connect is Simple: From 4-10 Protocols to 1

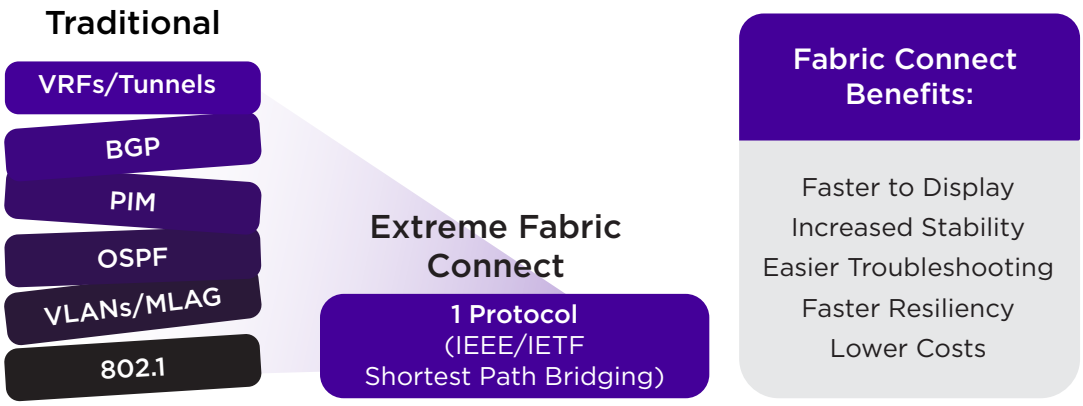

Figure 1: *The simplicity of Fabric Connect*

How Fabric Connect delivers dramatic simplification over traditional networks:

Traditional IP Networking	Fabric Connect
Built on multiple legacy protocols: MLAG, OSPF, BGP and PIM multicast	One protocol for all network services (L2/3 unicast, multicast, IPv4, IPv6)
Hop by hop provisioning, vulnerable to error	Edge only provisioning, error free
Network changes require planning and maintenance windows	Network changes completed on the fly due to never having to reconfigure the core/aggregation
Inconsistent recovery times ranging from sub-second to minutes	Sub-second failover and recovery
Separate wired and wireless administration	Unification of wired and wireless networking with dynamic auto-attach and common management, policies and analytics

An Inherently Secure Network that Can be Easily Segmented Into Secure Zones

In the past, OT network environments had little resemblance to corporate IT networks. Industrial Control Systems were completely isolated environments running proprietary control protocols and specialized hardware and software. However, with the shift of the operational environment away from proprietary devices and towards IP devices with common OS's (Windows), the OT environment is starting to resemble the IT environment. Although this presents an opportunity, by enabling more effective data collection and analytics from these OT systems, it also creates a significant security risk as these systems are no longer isolated.

According to the National Institute of Standards and Technology's Guide to Industrial Control Systems Security, network segmentation and segregation is one of the most effective architectural concepts that an organization can implement to protect its Industrial Control Systems. Fabric Connect, having originated in the service provider space, enables highly scalable virtual network segments to be deployed, with greater ease and with greater inherent security over traditional and next-generation approaches.

With Fabric Connect, tiers of segments can be created to isolate critical industrial control systems like supervisory control and data acquisition (SCADA), distributed control systems (DCS) and Programmable Logic Controllers (PLC), as well as critical physical safety applications such as video surveillance. Each service can be isolated in their own secure zone separate from the rest of the network services. This can be done at scale and without operational complexity. Because these systems can often be distributed across long distances (pipelines for example), network segments can extend seamlessly across the WAN and/or dark fiber infrastructures to ensure end to end isolation without operational complexity.

Because large numbers of network segments can be deployed, it is possible to isolate not only Industrial Control systems, groups of users (e.g. contractors) can also be isolated, as well as other IoT devices within the IT environment (building automation systems, IP cameras). Having a highly-segmented network reduces the attack surface and contains breaches to where they occurred, minimizing potential damage.

Fabric Connect is secure by design, and as a result is deployed in some of the most mission critical and highly secure environments in the world. It has also participated in numerous Hack-a-thon events in top tier universities, public events and top-secret government agencies - without a single breach to date.

Segmenting Traditional IP Networks	Segmenting Fabric Connect Networks
IP is ubiquitous by design and is based on an any to any forwarding paradigm where VLANs, ACLs, and/or firewalls are required to lock down communication to selected paths.	Fabric Connect is secure by design; services are based on circuit-like constructs that are completely isolated from one another unless otherwise provisioned. This reduces the number of ACLs/firewalls required since services are isolated automatically when configured.
Traffic forwarding is based on IP; network topology can be discovered, if breached, using IP scanning tools.	Traffic forwarding is based on Ethernet Switched Paths; therefore, the network topology cannot be discovered by IP scanning tools. This prevents lateral movement.
Network segmentation using a combination of VLANs, VRFs, ACLs and firewalls is cumbersome to deploy and lacks scale needed to support the proliferation of IIoT/ IoT devices.	Network segmentation is simple to deploy, highly scalable, highly secure and extends end to end across highly distributed oil and gas networks with ease.
Network segments are generally static and require manual provisioning when devices are disconnected and moved.	Network segments can extend and retract on demand as users, IIoT/ IoT devices connect and disconnect from the network. No residual configuration on edge ports.

Secure On-Boarding of Iot/IIot Devices with Efficient Processing of Iot/IIot Data

In addition to isolating critical Industrial Control Systems and other IoT devices in secure network segments, it is important to authenticate and on-board devices to the appropriate network segment efficiently, and securely.

Extreme's Network Access Control solutions apply granular controls over endpoints that are requesting on-boarding to the network. Specifically, they match endpoints with attributes, such as user, time, location, vulnerability, or access type, to create an identity. Role-based identities follow a user or IoT device, no matter from where or how it is connected to the network.

Another common characteristic of IoT/IIoT devices is that they only communicate with a very limited number of hosts. Therefore, applying whitelist policies that block all traffic unless it is to an authorized host, using only an authorized application or protocol, is an effective way to add an additional layer of security to these critical devices. This application of whitelist policies is yet another recommendation of the National Institute of Standards and Technology's Guide to Industrial Control Systems Security.

With device fingerprinting and device monitoring, it is possible to continually monitor the health of devices, ensuring that any device (or user) compromised with a virus, malware or even ransomware, is quickly identified and quarantined from the network, preventing its spread to other devices in the same network segment.

For IoT/ IIoT devices connecting into legacy network infrastructures, where an extra level of protection is needed, Extreme offers it's Defender for IoT solution. This solution acts as an overlay to the existing network – providing unique in-line protection of mission critical and/or vulnerable devices over any type of infrastructure (Extreme or 3rd party). It applies whitelist policies to control end device communication, securely on-boards devices to the network and isolates group of devices in their own IPSec encrypted tunnels that span from the device to the data center.

The proliferation of IoT/IIoT devices is also pushing the need for compute at the edge of the network. With highly distributed networks (connectivity to oil patches for example), that are often connected over low bandwidth links over a wide array of different types of wireless technologies, it is not often possible to achieve the desired latency for data processing when traffic is backhauled to a central data center. Extreme Networks switches are based on an Insight Architecture, which enables the ability to load virtualized applications that can run alongside the switch OS, enabling oil and gas companies to process data from their analog and digital sensors at the edge, and forward only relevant data back to the data center.

High Performance and Highly Reliable Multicast for Video Surveillance and Other Applications

In oil and gas, video surveillance is a major contributor to ensuring the safety of both workers and critical infrastructure. Today, smarter IP cameras provide greater capabilities beyond generating and transmitting video, they can also communicate with centralized management systems delivering video analytics output, alarms, and metadata alongside the video stream. These smarter video surveillance systems need the right network infrastructure to ensure the scale, performance and quality of the video.

Designed to simplify any video surveillance solution (IP, hybrid, unicast or multicast), Extreme Fabric Connect ensures that the network is ready to handle even the most complex nation-wide video surveillance deployments.

Some specific attributes of this solution include:

Video Surveillance/Multicast with Traditional IP Networking	Video Surveillance/Multicast with Traditional IP Networking
Built on multiple legacy protocols: MLAG, OSPF, and PIM multicast	One protocol for all network services (even multicast)
Complex provisioning: multicast provisioning on each router, rendezvous points, etc.	Edge only provisioning only. Minimal configuration.
Limited scale: hundreds of multicast streams limiting the number of cameras	Massive scale: tens of thousands of multicast streams for supporting massive camera deployments.
Erratic Performance: When a network event occurs, CPU spikes; sessions may drop	Predictable Performance: Eliminates CPU spikes.

Wi-Fi for Indoor, Outdoor, and Hardened Environments

As a leader in Gartner's wired and wireless LAN MQ, Extreme has one of the broadest wireless portfolios in the industry today. Whether it's for the highly distributed networks common for upstream exploration and production networks or the more condensed Wi-Fi deployments in midstream and downstream implementations, Extreme offers leading solutions that can be managed through the cloud or managed on premise.

Key capabilities of our wireless portfolio include:

- **AI-driven Wi-Fi architecture –** capable of self-organizing, self-learning, self-healing and self-optimizing in the most challenging environments.
- **Advanced security –** including fully stateful L2-L7 DPI firewall for context-based access security, Private Pre-Shared Key (PPSK) authentication, on-board RADIUS services, WIPS, VPN tunneling, and much more.
- **Programmable radios –** Software-defined dual 5 GHz radios monitor and automatically adjust Wi-Fi performance to achieve the highest levels of client performance and network optimization in challenging and demanding environments.
- **Automated Deployments –** Powered by cloud networking, access points can easily be deployed alongside thousands of others in no time at all. Extreme's management system provides granular templates and auto provisioning to enable centralized enterprise plug-and-play rollouts.
- **RF Monitoring –** Adaptive RF algorithms provide intelligent selection of the best channels and transmit power for unimpaired network access. Load balancing, band steering and many other attributes of the RF can all be automated.
- **APs suitable for harsh environments –** designed for extended temperature range and equipped with a watertight chassis, Extreme offers APs suitable for the tough environments common in the oil and gas industry.

End-to-End AI-Driven Cloud Management

Advanced data analytics, artificial intelligence (AI), cognitive automation, and machine learning are helping to convert the oil and gas industry's vast amounts of untapped data from sensors, PLCs, and other systems into actionable insights.

This same intelligence can also be applied to the network, through intelligent cloud-driven management. ExtremeCloud IQ, which is the next-generation management platform for Extreme's networking portfolio, analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and deliver new levels of network automation and intelligence.

ExtremeCloud IQ operates on Extreme's third generation Cloud Services architecture, capable of supporting millions of infrastructure devices and hundreds of millions of clients per each Regional Data Center. All Extreme Cloud Services components are hosted in secure SOC Type 1 data centers with 24/7 monitoring, scheduled backups, and build-in disaster recovery capabilities.

Key Attributes of ExtremeCloud IQ:

- **Flexibility** ExtremeCloud IQ is available in three deployment options to provide oil and gas companies with maximum flexibility.
  - **Extreme's public cloud** streamlines network operations with continuous updates, high availability, advanced machine learning analytics and insights, and anytime anywhere portal access.
  - **Extreme's private cloud** provides the same benefits as the public cloud solution but is deployed and maintained within a company's own datacenter.
  - **Extreme's local cloud** offers the same flexible architecture, but in a simplified and highly cost-efficient infrastructure deployed on-premises. This solution is ideal for small to mid-size organizations who want the power of the cloud, in addition, to complete control over their local deployment.
- **Agility –** Being a 3rd generation cloud platform, with an advanced microservices-based architecture, software development and deployment can occur in a continuous method, since updates can be done to individual services or collections of services to accomplish the enhancements without affecting the entire cloud infrastructure. This means that rather than rigid development schedules with only a few releases per year, with ExtremeCloud IQ, features and updates are delivered continuously – and without the need for complex service-impacting upgrades.
- **Security –** To ensure the highest levels of information systems and data protection, management, and compliance, Extreme's cloud platform is ISO/IEC 27001 certified by the International Standards Organization (ISO), complies with local data protection regulations such as GDPR, and is hosted within Amazon AWS data centers, taking advantage of AWS security and compliance capabilities at the data-center layer. Our cloud architecture is cloud-hosting agnostic, so is also capable of operating in Google, Azure, and even in a customer owned Data Center if needed.
- **Technology/Eco-system –** ExtremeCloud IQ offers a flexible infrastructure that can support both Extreme as well as third party infrastructure and applications creating a broad eco-system that can enable oil and gas companies to manage the best of breed technologies that are contained in their networks.

Summary

Extreme Networks is helping oil and gas companies across the globe digitally transform so that they can achieve their desired operational outcomes. We understand that the right network infrastructure is paramount in facilitating this transformation and that it assists in increasing efficiency, improving security and reducing costs. Extreme Network's Secure Automated Network Architecture achieves these objectives, helping oil and gas companies leverage AI, automation and big data to do more with less.

For more information on how Extreme Networks can help, please contact your local representative or visit www.extremenetworks.com.