2EVOLVE TECHNOLOGIES Future Ops 2021

2Evolve
TECHNOLOGIES

How We Started

Founded in 2003, by CEO Cindy Ried

- The vision was surrounded by the idea of shaping strong relationships that forms real revenue and business growth in the fast and complex world of IT
- With over 75 business partners (and growing), who are each highly skilled within their areas of expertise
- 2Evolve was build on a foundation of a knowledgeable team of consultants who are still here today, nearly two decades later

Headquarters based in Omaha, NE

- With additional branch offices in St. Louis, MO, Springfield, MO, and Grand Junction, CO
- 2Evolve Technologies has evolved into a premier technology partner offering over 200 vendor solutions
- Our commitment to superior customer service and cutting-edge solutions ensures your technology needs are met with industry experts and excellent ongoing support
- Ongoing/back office support, with nearly two decades of experience that gives every one of our partners and customers a superior customer experience
- 2Evolve Technologies now manages over 6,000 clients & our base continues to grow daily

2Evolve TECHNOLOGIES

LUMEN

Solutions We Offer

UCaaS

BASIC UCAAS SEAT
- Voice
- Text / SMS
- Video (Zoom)
- Web Conferencing
- Collaboration (Slack, Glip, MS Teams, etc.)

ADD ONS
- CRM Integration
- Accounting Integr.
- CCaaS Integration
- IVR
- Call Recording
- AI / Sentiment

PREMISE SYSTEMS
- Prem as-a-Service
- SIP Trunks

CCaaS

CCAAS SOLUTION
- IVR
- Analytics
- Performance Mgmt
- Dashboards

DIALER
- Outbound Dialer
- Preview
- Predictive Dialer
- Progressive Dialer

WORKFORCE MGMT

QUALITY MGMT
- AI / Sentiment

CRM INTEGRATIONS

UCAAS INTEGRATIONS

PCI HANDLING

HIPPA HANDLING

GAMIFICATION

ADD ONS
- Accounting Integr.
- Call Recording

Network

SD-WAN
- Auto-Failover
- Bonding
- Intelligent Routing
- VNF (Virtual Network)
- Firewall
- Application Aware

CONNECTIVITY
- Broadband
- Dedicated Fiber
- Coax
- WISP / Microwave
- 3G/4G/5G Internet
- Satellite Internet
- Circuit Aggregation

MANAGED WIFI
- Internal Network
- Guest Network

SECURITY
- Firewall (Prem / Web)
- Endpoint Security
- Network Security Assessment

REMEDIATION
- Circuit Monitoring
- Trouble Ticket Creation

Security

IDENTIFY
- Virtual CISO
- Cyber Consulting
- Vulnerability Assess.
- Penetration Test
- Compliance
- Phishing Simulation
- Awareness Training

PROTECT
- Managed Firewall
- Web Security
- Email Security
- Endpoint Protection
- Managed Cloud FW
- Data Protection
- Zero-Trust Framework
- Remote User VPN
- Patch Management

DETECT
- Log Mgmt (SEIM)
- AI Machine Learning
- Intrusion Detection
- Intrusion Prevention
- SOC as a Service

RESPOND
- Incident Response
- Containment / Eradication / Restore

Cloud

CONNECTIVITY
- Public Cloud Onramps
- Direct Connects
- Express Routes

COMPUTING
- Private Cloud
- Public Cloud
- Bare Metal
- Colocation
- Orchestration

IAAS

STORAGE
- Cloud File Storage
- Colocation
- Managed Backup
- Disaster Recovery

MANAGED SVCS
- Managed O365
- IT Support
- Desktop aaS
- Cloud Migration
- Professional Svcs

SAAS MGMT
- Microsoft Office
- SAP

IoT

SENSORS
- Temperature
  - Pressure
  - Soil Moisture Content
  - Video
- Panic Buttons
- Preventive Maintenance
-Bin/Tank Monitoring
- Occupancy

FLEET & ASSET TRACKING
- Cold Chain Monitoring
- AI for Driver Behavior
- Cargo Monitoring
- Supply Chain Management
- Indoor Tracking

REPORTING
- Geo-Fence
- Detailed Use
- Velocity / Acceleration
- Compliance

Misc.

MOBILITY
- Handsets
- iPads
- Devices

MOBILE NETWORK
- Detail Reporting
- Device Usage Mgmt
- Application Filtering
- Detailed Reporting
- CyberReef Solutions

EXPENSE MGMT
- Wireline
- Mobility

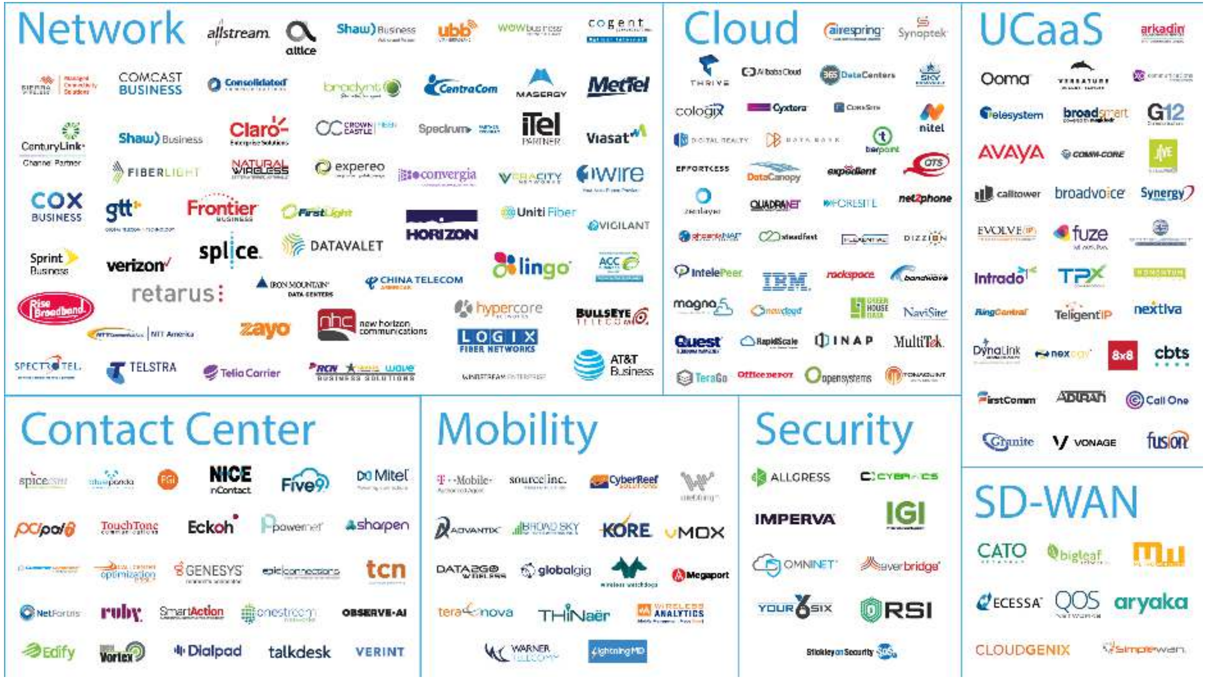
PHYSICAL SECURITY
- Video Surveillance
- Access Cards

SURVEYS
- Ariel Drone Surveys ConnexiCore

ANSWERING SVCS
- Ruby Receptionist

2Evolve TECHNOLOGIES

LUMEN



Suppliers We Offer

© 2020 Lumen Technologies. All Rights Reserved.

2Evolve TECHNOLOGIES

LUMEN®

Our Team. Our Mission. Ou
Vision. Our Goal.

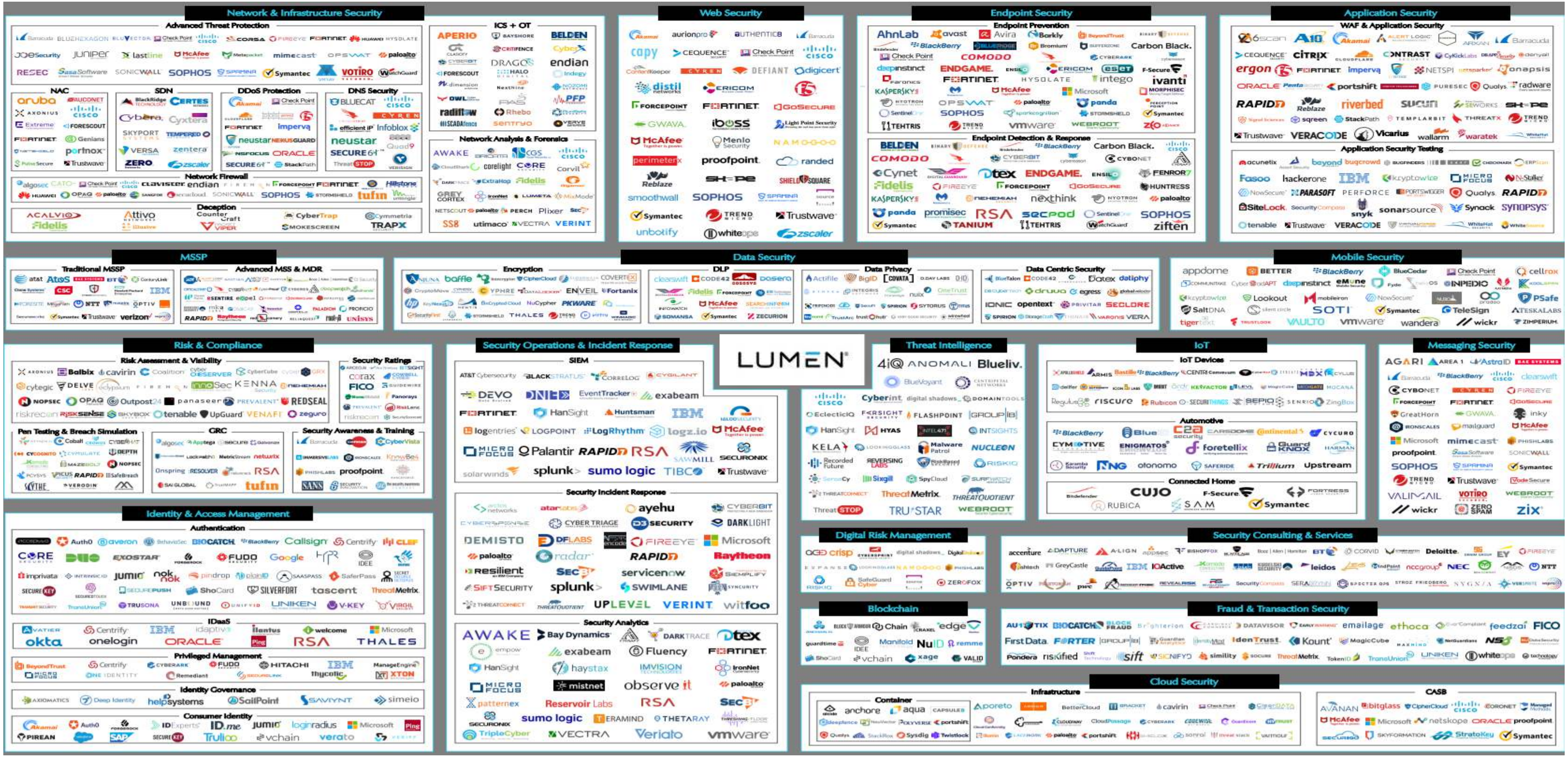
- **Our Team:** is our biggest asset
  - With over 100 years of combined experience (some of our team has been with us since we started in 2003), we are unstoppable
- We support one another in every way so we can make our customer and partner experiences the absolute best possible
- Each of us at 2Evolve seek integrity at the highest level and this means we are completely translucent to all customers and partners
  - This is the key to all relationships and how our company has thrived for almost two decades

- **Our Mission:** Provide premier IT & Carrier solutions from leading Global IT communications companies.
- **Our Vision:** To be regarded as the premier communications and technology group for all Cloud, Data Center, Network, Mobility, and Business Intelligence solutions.
- **Our Goal:** To provide customers with the best possible solutions to meet their business needs. Your satisfaction is our indicator for success

2Evolve
TECHNOLOGIES
LUMEN®

Lumen Security

Presenting A Broad Portfolio of Lumen Security Service:
JT Lecompte + Rob Browning


Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
ICS + OT
Network Analysis & Forensics
Network Firewall
Deception
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Operations & Incident Response
SIEM
Security Incident Response
Security Analytics
LUMEN
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting & Services
Blockchain
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB

LUMEN

LUMEN

Lumen® Security Sneak Peek Presented in valued Partnership with 2Evolve Technologies

Date: October 15th 2021

Uncover vulnerabilities fast

Technology without borders

Have you checked your network vulnerabilities lately?

- **Hybrid/remote workers opening new vulnerabilities.** Colonial Pipeline attack was through old VPN credentials.
- **Ransomware attacks on the rise.** 2021 attacks include: Colonial Pipeline $4MM, JBS Foods $11MM, Acer computers $50MM.
- **Company credentials you may not know are exposed are being sold on the Dark Web.** Have you ever wondered what a hacker can see when researching your company?

Security Sneak Peek

Uncover vulnerabilities fast

See what hackers see within a short amount of time and get a report stating known vulnerabilities. You also receive a one-time service credit of up to $5,000 to purchase eligible security services

- Dark Web Scan
- Technical Scan
- Web Application Scan
- Recommendation from world-class security experts on how to improve your risk exposure
- Up to a $5,000 credit toward the new purchase of eligible security services*

Take a sneak peek and fight back

Uncover vulnerabilities fast

Dark Web Scan

- Uncover any exposed credentials on the Dark Web on your current domains (up to 5 domains)

Technical Scan

- Identify weaknesses in your organization’s public facing environment (up to 100 external IP addresses)

Web Application Scan

- Pinpoint web application vulnerabilities (limited to 2 web apps)

Assessment Report

- After the scans are completed, Lumen security analysts deliver a report that summarizes the methodology, the findings and our recommendations
- The assessment will be delivered within 30 days of project kickoff

Security Credit

- Receive a one-time service credit up to $5,000 for the new purchase of eligible security services*

*Offer requires customer to purchase and complete a qualifying Lumen Security Assessment. After assessment completion, customer will be eligible for a one-time service credit to be used within one-year of assessment completion in the amount of customer’s monthly recurring or non-recurring service charge up to $5,000, for the new purchase of eligible security services with a minimum 12-month term agreement for services billed monthly or with a minimum $10,000 non-recurring charge for services billed one time. The one-time service credit will be applied to customer’s account within 30 days after the first month following installation and billing of all eligible services. Offer excludes charges for equipment, installation, taxes, fees and surcharges. Early termination fees will apply as set forth in customer’s agreement and include an amount equal to any service credits received under this offer. Service and offer may not be available everywhere. Lumen may change, cancel or substitute offers and services, or vary them by service area at its sole discretion without notice. Credit approval and deposit may be required. Offer may not be combined with other offers. 30-day timeline depends on customer promptly providing all info and access requested by Lumen. Additional restrictions, terms and conditions apply.

Uncover what’s hidden on the Dark Web and more

Know Your Biggest Vulnerabilities

- Three-part vulnerability scan
- Detailed analysis received within 30 days of project kickoff
- Strengthen your security posture

Customized Reporting Based on Today’s Market

- Assess your immediate risks
- Learn what’s exposed within 30 days of project kickoff
- Receive credit for future services

Learn from the Experts

- Decades of cybersecurity experience
- Experts in delivering security assessments

Sneak Peek Assessment Report

Lumen Security "Sneak Peek" Assessment for Acme, Inc. a subsidiary of ABC Co.

07/16/2021

This document is CONFIDENTIAL and PROPRIETARY. It is intended solely for the internal use of the customer to whom it was provided.

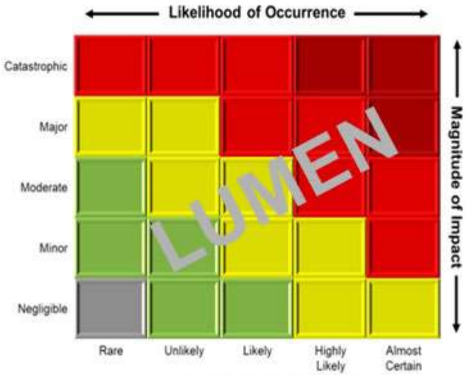
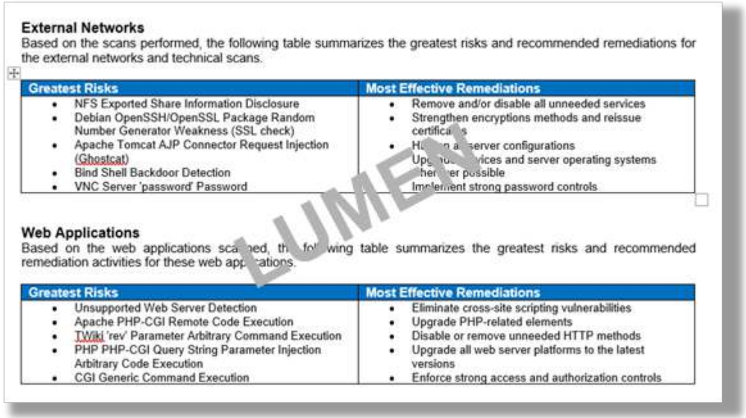


Figure 2: Overall Risks - Heat Map



External Networks

Based on the scans performed, the following table summarizes the greatest risks and recommended remediations for the external networks and technical scans.

Greatest Risks	Most Effective Remediations
• NFS Exported Share Information Disclosure • Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) • Apache Tomcat AJP Connector Request Injection (Ghostcat) • Bind Shell Backdoor Detection • VNC Server 'password' Password	• Remove and/or disable all unneeded services • Strengthen encryptions methods and reissue certificates • Harden all server configurations • Upgrade devices and server operating systems wherever possible • Implement strong password controls

Web Applications

Based on the web applications scanned, the following table summarizes the greatest risks and recommended remediation activities for these web applications.

Greatest Risks	Most Effective Remediations
• Unsupported Web Server Detection • Apache PHP-CGI Remote Code Execution • TWiki 'rev' Parameter Arbitrary Command Execution • PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution • CGI Generic Command Execution	• Eliminate cross-site scripting vulnerabilities • Upgrade PHP-related elements • Disable or remove unneeded HTTP methods • Upgrade all web server platforms to the latest versions • Enforce strong access and authorization controls

Dark Web Scan

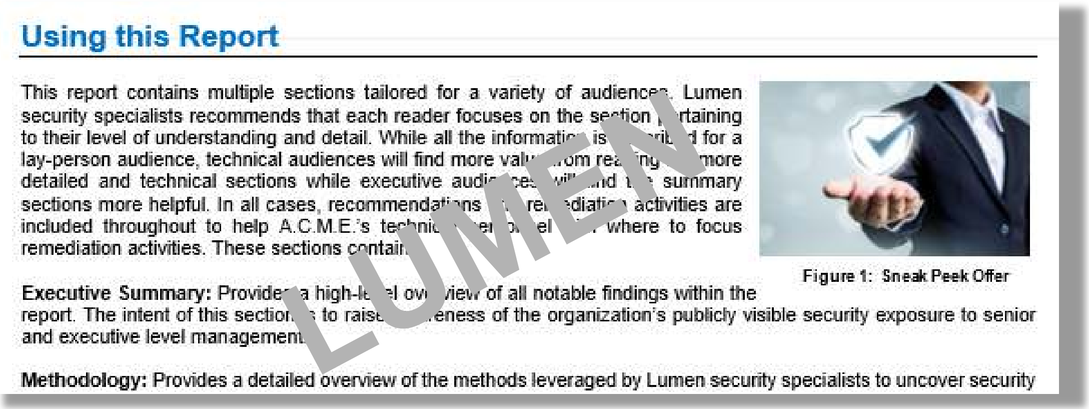
By its very nature, information obtained via publicly accessible sources must be considered already compromised, or at the very least unsuitable for use in authentication methods. As a result, Lumen security specialists recommend that any information uncovered through these avenues never be used for security controls.

While it is unreasonable to suggest any security measure to processes and systems outside of A.C.M.E.'s control, Lumen security specialists recommend the following actions:

- Do not re-use passwords
- Use complex passwords
- Utilize all available email and DNS security capabilities

Figure 3: Implementing Security Best Practices

Sneak Peek Assessment Report



Using this Report

This report contains multiple sections tailored for a variety of audiences. Lumen security specialists recommends that each reader focuses on the section pertaining to their level of understanding and detail. While all the information is described for a lay-person audience, technical audiences will find more value from reading the more detailed and technical sections while executive audiences will find the summary sections more helpful. In all cases, recommendations and remediation activities are included throughout to help A.C.M.E.'s technical personnel on where to focus remediation activities. These sections contain:

Figure 1: Sneak Peek Offer

Executive Summary: Provides a high-level overview of all notable findings within the report. The intent of this section is to raise awareness of the organization's publicly visible security exposure to senior and executive level management.

Methodology: Provides a detailed overview of the methods leveraged by Lumen security specialists to uncover security

Network Security Details

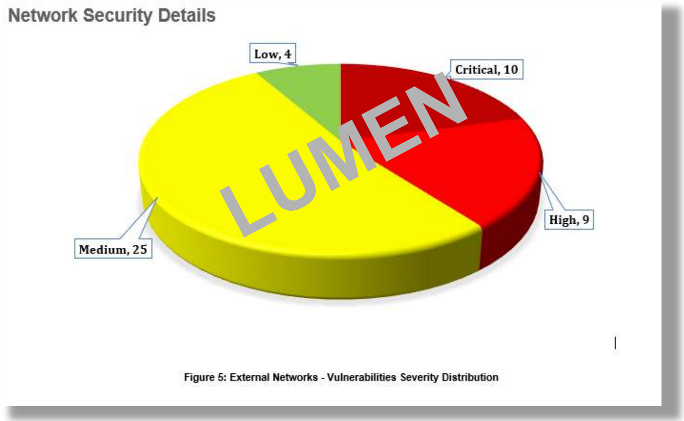


Figure 5: External Networks - Vulnerabilities Severity Distribution

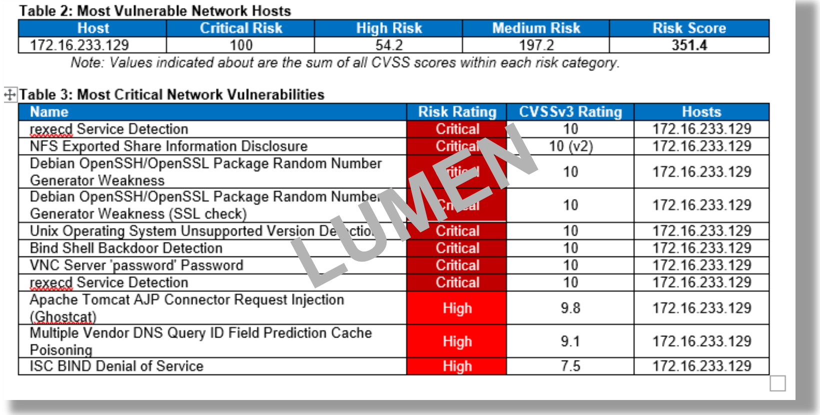


Table 2: Most Vulnerable Network Hosts

Host	Critical Risk	High Risk	Medium Risk	Risk Score
172.16.233.129	100	54.2	197.2	**351.4**

Note: Values indicated about are the sum of all CVSS scores within each risk category.

Table 3: Most Critical Network Vulnerabilities

Name	Risk Rating	CVSSv3 Rating	Hosts
rexecd Service Detection	Critical	10	172.16.233.129
NFS Exported Share Information Disclosure	Critical	10 (v2)	172.16.233.129
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Critical	10	172.16.233.129
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Critical	10	172.16.233.129
Unix Operating System Unsupported Version Detection	Critical	10	172.16.233.129
Bind Shell Backdoor Detection	Critical	10	172.16.233.129
VNC Server 'password' Password	Critical	10	172.16.233.129
rexecd Service Detection	Critical	10	172.16.233.129
Apache Tomcat AJP Connector Request Injection (Ghostcat)	High	9.8	172.16.233.129
Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	High	9.1	172.16.233.129
ISC BIND Denial of Service	High	7.5	172.16.233.129

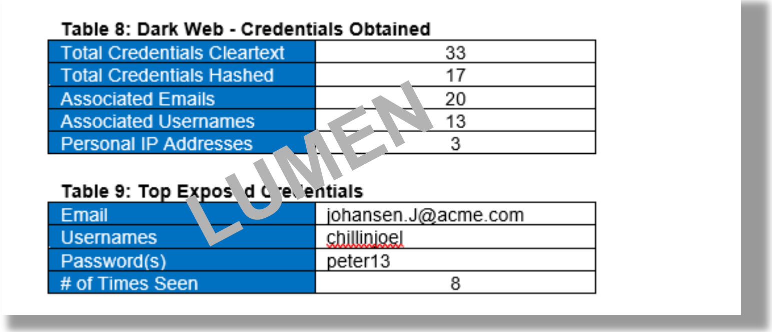


Table 8: Dark Web - Credentials Obtained

Total Credentials Cleartext	33
Total Credentials Hashed	17
Associated Emails	20
Associated Usernames	13
Personal IP Addresses	3

Table 9: Top Exposed Credentials

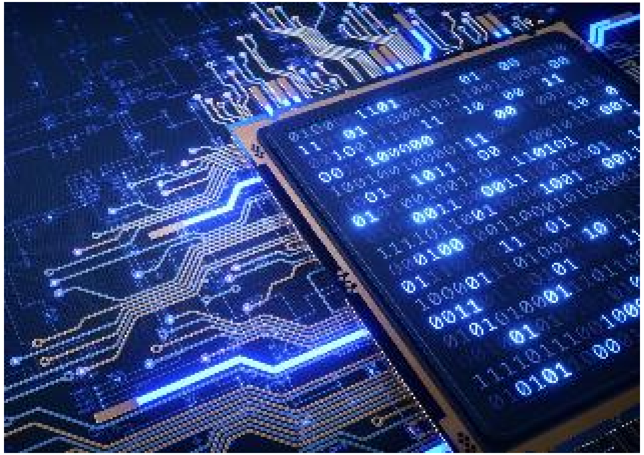
Email	johansen.J@acme.com
Usernames	chillinjoel
Password(s)	peter13
# of Times Seen	8

Threat intelligence you can count on

BLACK LOTUS LABS®

Powered by Black Lotus Labs®

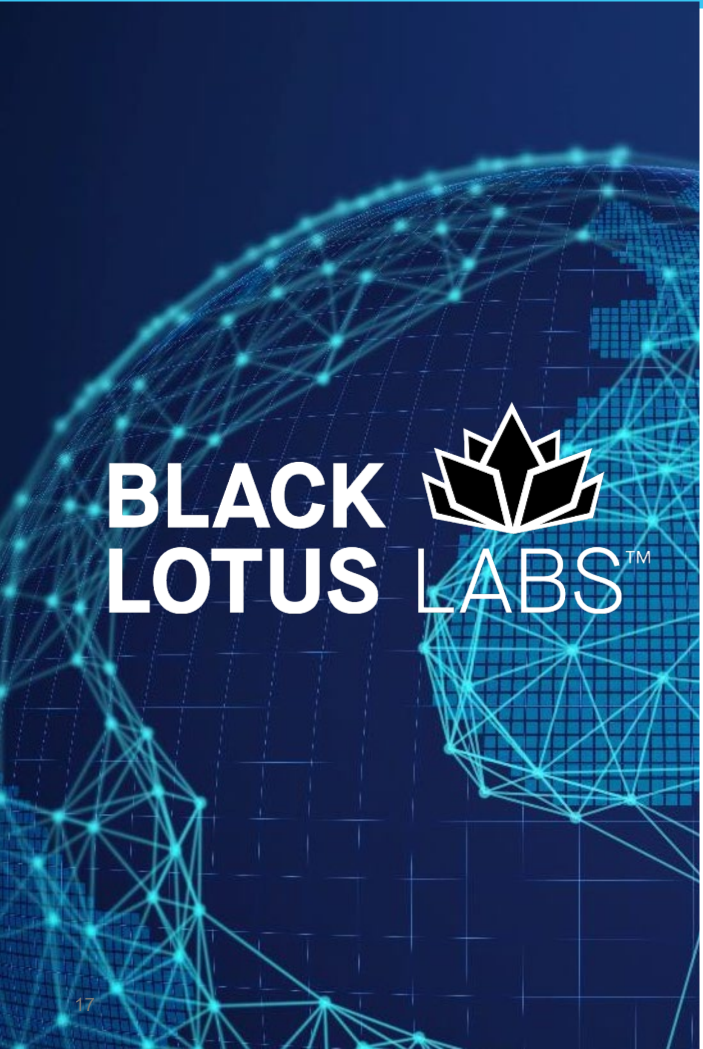
- **Threat Intelligence built from one of the world’s largest internet backbones**, which gives us a massive field of view when it comes to emerging and evolving cyber threats
- **Comprised of threat intelligence experts and data scientists** that create accurate, rapid and actionable threat intelligence for Lumen customers, products and services
- Your vulnerability scanning is being **conducted by a world-class security team** providing some of the most comprehensive threat intelligence in the world



Black Lotus Labs defends the internet against known and emerging threats, discovers new attack vectors, and indirect threats in the wild before they can harm your organization.

Lumen DDoS Mitigation Services Presented with 2Evolve Technologies

Date: October 15th 2021



Lumen Security:
See More – Stop More – in Real-time

- Global network provides expansive visibility into threat landscape
- Custom, high-fidelity threat intelligence
- Disrupting malicious infrastructure with proactive botnet takedowns
  - Discover ~680+ C2s per month
  - Track~28,000 C2s daily
  - Take down ~63 C2s per month
- Investing in simplicity, digital experience, automation
- Creating a safer Internet through information sharing and collaboration

Why Lumen for DDoS?

1

Global Peering/Carrier Agnostic

120+ Tbps of global network capacity, localized private peering w/ private interconnects maximizes performance - more than **9,000 unique AS interconnects***

2

First Line of Defense

Internet Backbone as a Layer of Defense – **85 Tbps of FlowSpec defense capacity**, provides additional layers of mitigation against volumetric layers 3 & 4 attacks

3

Tiered Scrubbing Architecture

Escalated to Super or Regional centers when thresholds exceeded, **reduces collateral damage**

4

Botnet Takedowns + Rapid Threat Defense

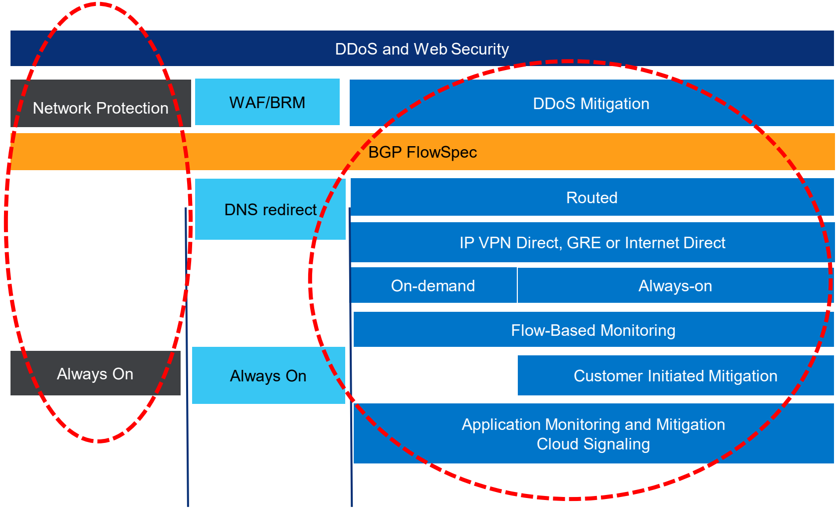
Black Lotus Labs **removes ~63 C2s monthly** from the Lumen network, less malicious traffic hitting customer firewalls. Rapid Threat Defense blocks bot traffic before it hits a scrubbing center.

* Telegeography, *Global Internet Geography Executive Summary*, 2020

Selecting the right DDoS Mitigation Service

Assets protected

- Website
- Data center
- Corporate offices
- Public or private cloud environment



Type of mitigation

- Always-on
- On-demand

Methods of clean traffic return delivery

- Over the top
- Integrated with the internet circuit
- Via private connectivity

Attack monitoring

- Provider-monitored
- Customer-monitored

Mitigation control

- Customer-initiated
- Automated
- SOC-assisted

LUMEN®

Internet backbone as a layer of defense

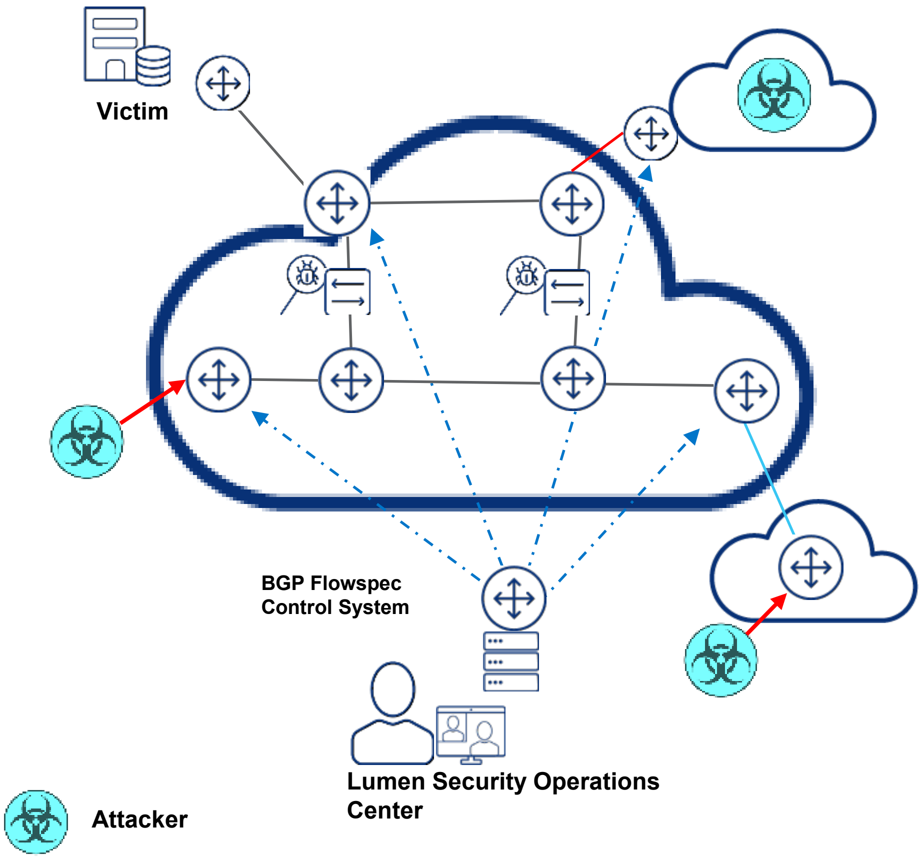
BGP Flowspec Capability

- Uses BGP Flowspec announcements for an automated ACL rules delivery to Flowspec capable routers across the backbone and edges

- Highly scalable global solution

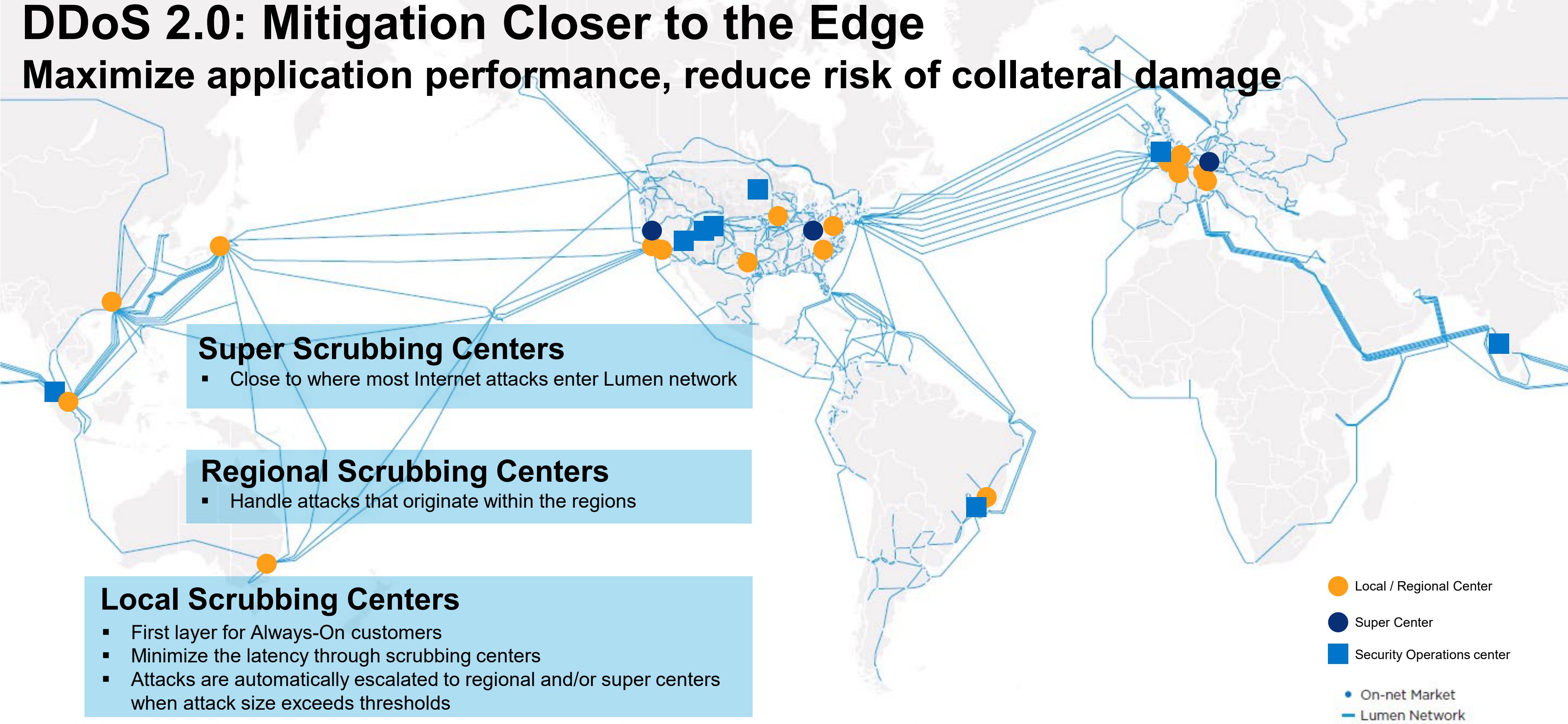
- Facilitates emergency mitigation.

- **Key Benefit:** Rapid deployment of rules globally
  - Provides an additional layer of mitigation against large scale volumetric layers 3 and 4 attacks



DDoS 2.0: Mitigation Closer to the Edge

Maximize application performance, reduce risk of collateral damage



Super Scrubbing Centers

- Close to where most Internet attacks enter Lumen network

Regional Scrubbing Centers

- Handle attacks that originate within the regions

Local Scrubbing Centers

- First layer for Always-On customers
- Minimize the latency through scrubbing centers
- Attacks are automatically escalated to regional and/or super centers when attack size exceeds thresholds

© 2020 Lumen Technologies. All Rights Reserved. Map information above is current as of July 2020. Information is subject to change. Contact Lumen for updates or details. The Lumen global network is made up of owned, leased access and IRU segments, which are not distinguished on this map. Lumen engages in-region carriers to provide services in some markets.

LUMEN®

Permanent rules on the Network Edge

- **Facilities-based Internet services providers** can add permanent network defense rules on the provider edge routers
- Base foundation in a multi-layered approach to DDoS mitigation: it helps reduce the attack surface
- Complements traditional DDoS mitigation service
- Delivered via Network Protection Service

Key Attributes

- Always-on security control
- Layers 3-4 volumetric attack mitigation
- IPv4 or IPv6 filters, rate limiters, null routes and permanent ACLs
- Additional ACLs on upstream internet backbone routers
- Flow-based monitoring for advanced reporting

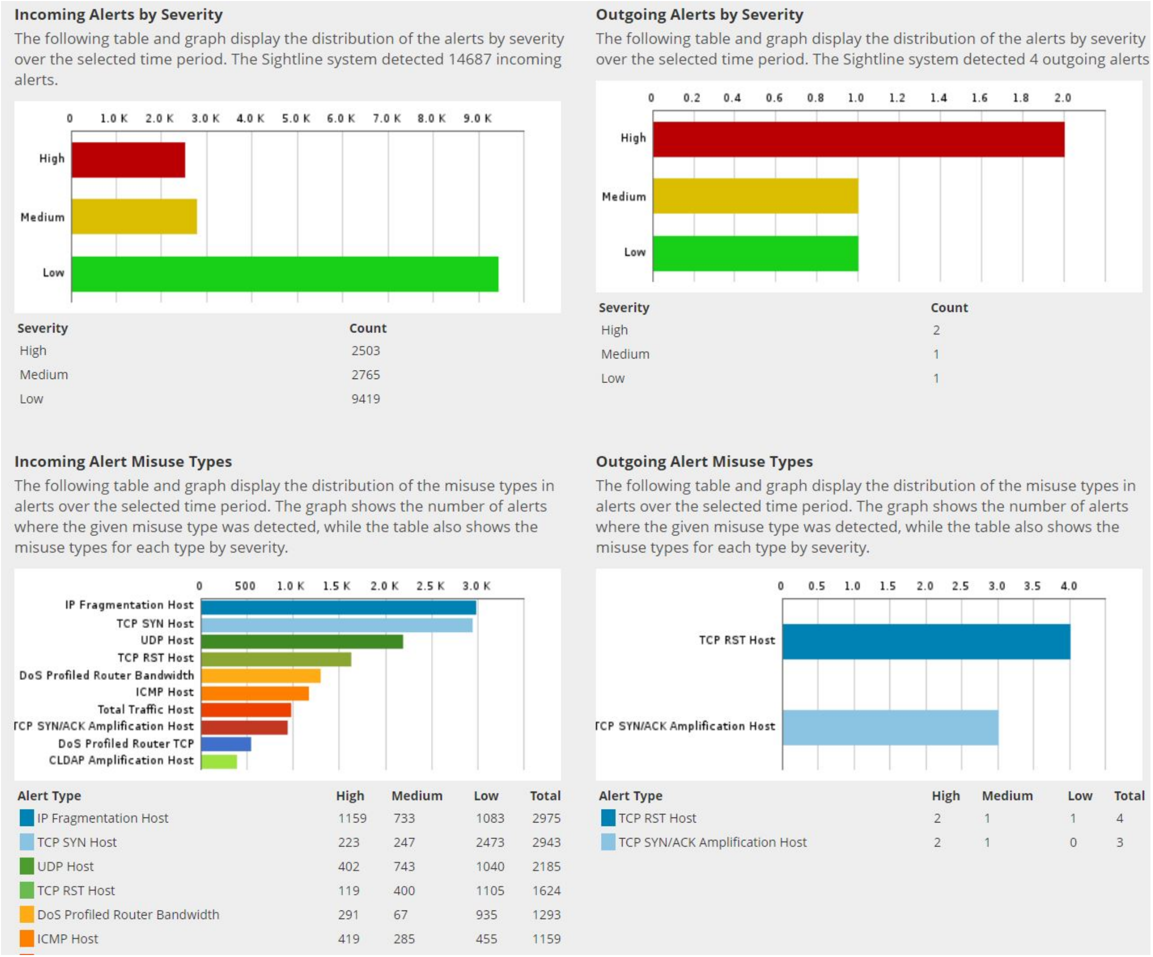
Lumen® DDoS Mitigation with Rapid Threat Defense

Enables immediate, automatic blocking of attack traffic

- Rapid Threat Defense blocks immediately; a typical advanced scrubbing algorithm can take a minute from detection to blocking.
- Black Lotus Labs threat intel refreshed every 15 minutes
- Increases the data available beyond network-behavioral and vendor-native intelligence
- Integrates and orchestrates threat discovery, correlation, policy and response to automate preventative action
- Expands categories of threat for Lumen DDoS platform response
- High fidelity data: proprietary algorithms plus original threat discovery based on machine learning and Lumen honeynet technologies

Real-Time Reporting Portal

Peacetime performance and event reporting with extensive attack visibility and historical threat data



Incoming Alerts by Severity

The following table and graph display the distribution of the alerts by severity over the selected time period. The Sightline system detected 14687 incoming alerts.

Severity	Count
High	2503
Medium	2765
Low	9419

Outgoing Alerts by Severity

The following table and graph display the distribution of the alerts by severity over the selected time period. The Sightline system detected 4 outgoing alerts

Severity	Count
High	2
Medium	1
Low	1

Incoming Alert Misuse Types

The following table and graph display the distribution of the misuse types in alerts over the selected time period. The graph shows the number of alerts where the given misuse type was detected, while the table also shows the misuse types for each type by severity.

Alert Type	High	Medium	Low	Total
🟦 IP Fragmentation Host	1159	733	1083	2975
🟦 TCP SYN Host	223	247	2473	2943
🟩 UDP Host	402	743	1040	2185
🟩 TCP RST Host	119	400	1105	1624
🟧 DoS Profiled Router Bandwidth	291	67	935	1293
🟧 ICMP Host	419	285	455	1159

Outgoing Alert Misuse Types

The following table and graph display the distribution of the misuse types in alerts over the selected time period. The graph shows the number of alerts where the given misuse type was detected, while the table also shows the misuse types for each type by severity.

Alert Type	High	Medium	Low	Total
🟦 TCP RST Host	2	1	1	4
🟦 TCP SYN/ACK Amplification Host	2	1	0	3

LUMEN

Lumen Global Security Operation Centers (SOCs)

Robust visibility and support

- With 8 locations across North America, APAC, EMEA and Latin America, we protect our customers 24/7.
- The same global team charged with protecting Lumen’s global infrastructure is monitoring and managing your security services.
- Our global network provides extensive visibility into threats – our SOC leverages this information to protect your assets.
- As a global ISP, we absorb large-scale attacks as part of the day-to-day operation of our global IP infrastructure.

Why Lumen Security?

At Lumen, we **see more to stop more** threats – **in real-time**. Our global network backbone provides vast visibility into the threat landscape to power our portfolio of security solutions.

Our portfolio provides the ingredients that **secure the Lumen platform**, applications and data **at the edge** and a **digital buying experience**.

We help organizations **simplify security** by embedding protection in network services and automating threat detection and response. We provide original **high-fidelity threat intelligence**, expert consulting and a robust professional services practice to empower today's defenders.

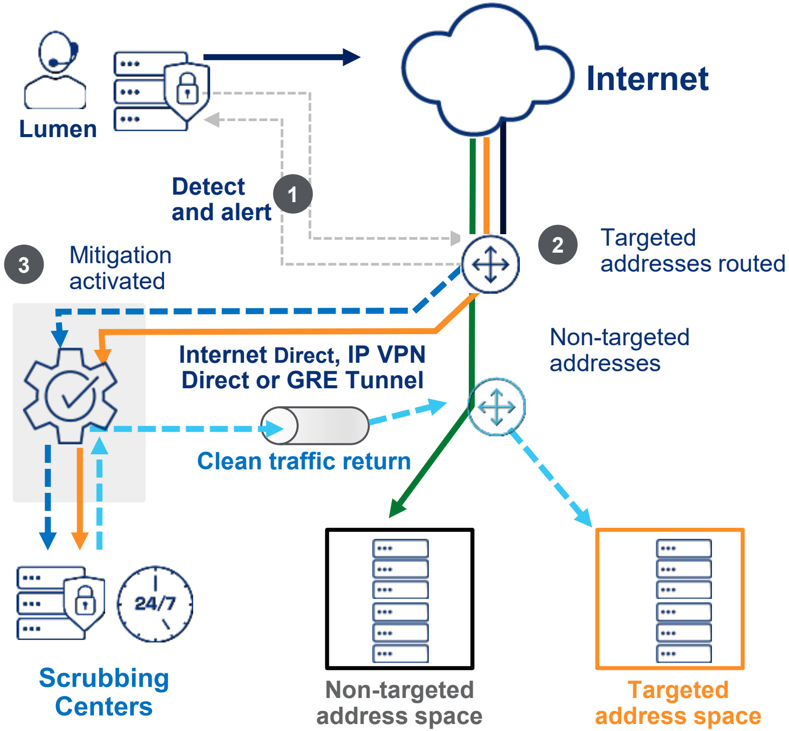
Questions?
Appendix for Technical Detail

Lumen® DDoS Mitigation Service

1. **Detection:** Attack identified by Customer or Lumen
2. **Targeted Addresses Routed:** Traffic routed and scrubbed based on service type: Always-on, and on-demand
3. **Mitigation:** Targeted address traffic diverted and scrubbed
4. Command & Control server take-downs performed as appropriate

Service Highlights

- Network-based, unlimited mitigation
- Always-on, on-demand, and options
- Route determined by BGP configuration
- Asymmetric traffic flow
- Private connection for forwarding clean traffic
- Volumetric and application layer attack mitigation (Layers 3-7)
- Optional Flow-Based Monitoring (proactive monitoring and alerting)



Clean Traffic Return: Internet Direct Option

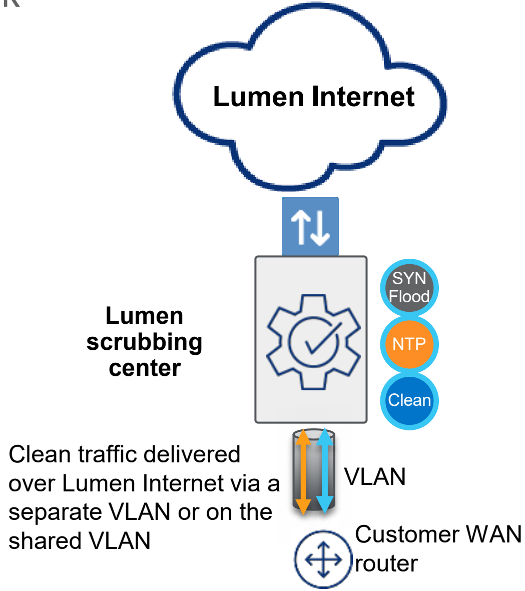
Clean traffic return using VLAN trunking over the Lumen IP network

Efficiency and Reliability

Utilize Lumen Internet

Bandwidth and Capacity

- Lumen® Internet service only
- Delivery of clean traffic over Lumen Internet circuit via a separate VLAN or on the same VLAN logical that also delivers the Internet traffic
- Only limitation of clean traffic return is the size of the internet circuit (i.e., up to 100 Gbps)
- Available with always-on, or on-demand
- Prioritization of clean traffic return over other internet traffic provides efficiency and performance
- VLAN trunks are more reliable than GRE tunnels



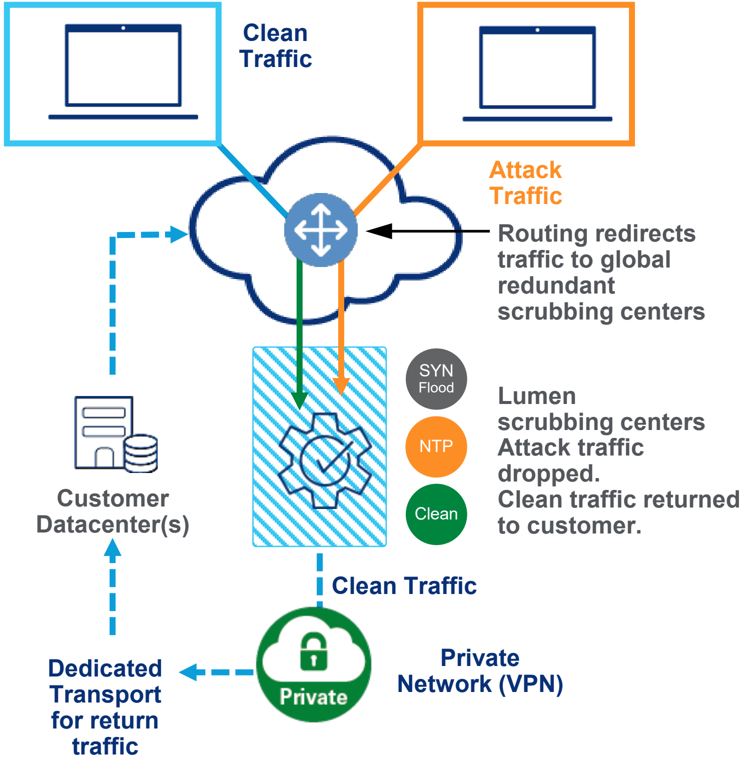
Clean traffic delivered over Lumen Internet via a separate VLAN or on the shared VLAN

Clean Traffic Return: IP VPN direct options

Uses IP VPN as a forward path from Lumen scrubbing centers to customer data center for clean traffic

Simplified Management	Performance and Reliability	Bandwidth and Capacity

- Provides a more reliable solution when compared to GRE tunnel for forwarding clean traffic.
- Eliminates the need to maintain GRE tunnels to multiple scrubbing locations.
- Available with always-on or on-demand
- No need to adjust TCP MSS, which can have negative impact on certain applications.
- Reduces latency and jitter for clean traffic compared to best effort through GRE tunnel over public Internet.
- Lower cost compared to pure play providers for similar solution when location has Lumen IP services

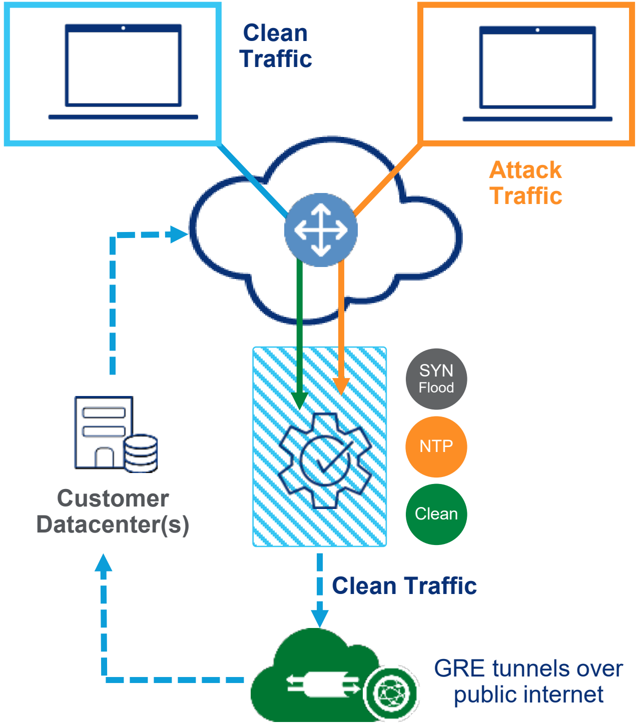

Clean Traffic
Attack Traffic
Routing redirects traffic to global redundant scrubbing centers
SYN Flood
NTP
Clean
Lumen scrubbing centers Attack traffic dropped. Clean traffic returned to customer.
Customer Datacenter(s)
Clean Traffic
Private
Private Network (VPN)
Dedicated Transport for return traffic

Clean Traffic Return: GRE option

Uses GRE tunnels over public internet as a forward from Lumen scrubbing center to customer data center(s) for clean traffic

Service Highlights

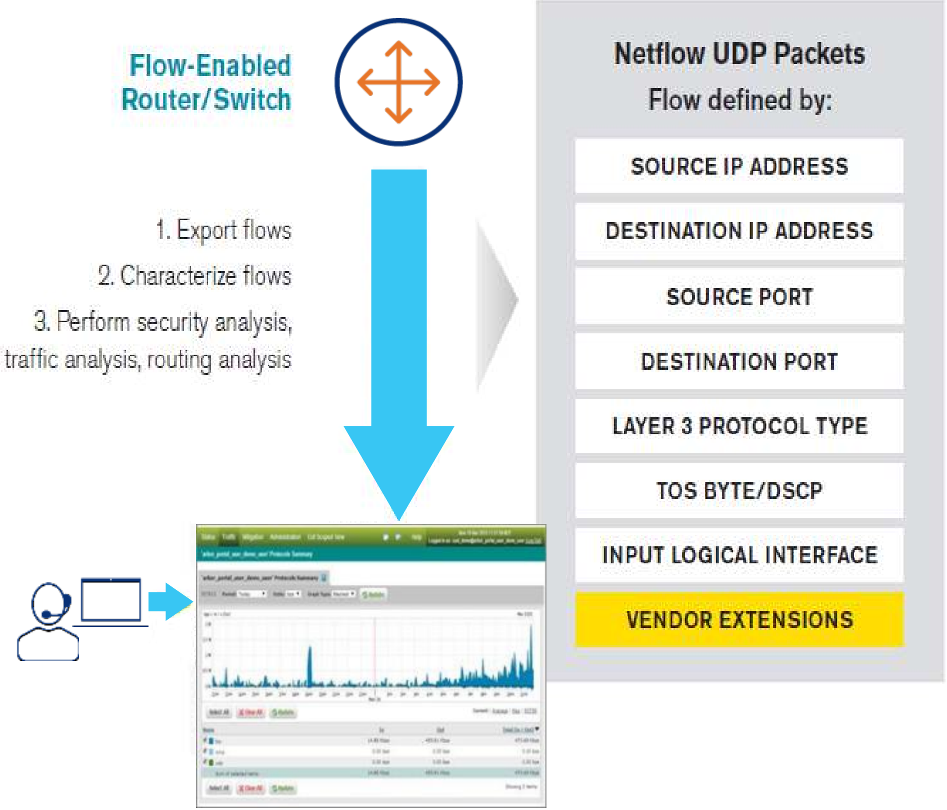
- Network-based, unlimited mitigation
- Always-on, or on-demand options
- Route determined by BGP configuration
- For customers with a maximum of 3 Gbps of peak inbound clean traffic
- Volumetric and application layer attack mitigation (Layers 3-7)
- Optional Flow-Based Monitoring (proactive monitoring and alerting)
- Carrier-agnostic delivery
- Available for emergency turn-up



Flow-based monitoring option

Proactive monitoring and alerting

- Monitors customer edge or Lumen routers and detects anomalies and changes in volumetric flows
- Detects layer 3 and 4 DDoS attacks and provides alerts to Lumen SOC and customer
  - Netflow, Sflow, Jflow (Requires SNMP access)
- 24/7 monitoring and alerts backed by SLAs
- Additional forensic evidence for faster mitigation
- Available as an option with DDoS Mitigation service and Network Protection Service



Increased Flexibility With Customer Initiated Mitigation

Enabling customer-initiated BGP route control functionality

- Optional feature: Initiate mitigation via the route announcement to Lumen rather than calling the Lumen Security Operations Center
- Reduce interactions between our Security Operations Center and your security teams
- Available to “always-on” GRE, Internet Direct, and IP VPN Direct customers.
- Dynamically advertise the preferred prefixes into the clean return tunnels
- The advertised prefixes automatically propagate from the Lumen scrubbing infrastructure to the Internet
- Lumen® DDoS Mitigation Service automatically begins scrubbing advertised traffic
- Traffic load sharing (not balancing) is supported for customers with diverse connectivity from the same site

LUMEN®

DDoS Mitigation offer

PRICING STRUCTURE

Protected Address Space

- Up to a total of 256 blocks of /24 IPv4 or /48 IPv6 included
- Unlimited Protected Subnets (Fixed MRC, NRC)

Clean Traffic Return

- Bandwidth
- MRC
- NRC

Service Type

- Always-on
- On-demand
- GRE / IP VPN Direct / Internet Direct

Optional add-on components

- Flow-Based Monitoring (Fixed MRC, NRC)
- Cloud Signaling (Fixed MRC, NRC per device) - Requires DDoS mitigation appliance at customer’s location
- Emergency Turn-up (NRC)

Lumen® DDoS Hyper-DDoS Mitigation Service Feature Comparison:

Features		DDoS Hyper	DDoS Mitigation Service
Self-Serve via Portal		✓	
Type of Mitigation	Always-On		✓
	On-Demand	✓	✓
Clean Traffic Return Method	Over the Top/GRE – Lumen* or Third Party	✓	✓
	Integrated with Internet Circuit		✓
	Private Connectivity (IP VPN)		✓
Attack Monitoring	Lumen Network		✓
	Customer CPE	✓	✓
Attack Size Mitigation	Unlimited	✓	✓
Mitigation Control	Automated	✓	✓
	Customer-Initiated		✓
	SOC-Assisted	✓	✓
Global SOC Support 24/7	Protection against most common attacks with basic customization	✓	✓
	Full customization for attack mitigation		✓
	Priority handling		✓
IP Protection	IPv4	✓	✓
	IPv6		✓
Rapid Threat Defense	Black Lotus Labs-provided countermeasures	✓	✓
Contract and billing currency	U.S. only	✓	✓
	Global, with some restrictions		✓
Professional Security Services Assistance	Optional, designated security consultant for runbooks, analysis and reporting tailored to customer business needs	✓	

*Not supported by Lumen Managed Router

Questions?