Internet2 NET+ Security and Identity Portfolio

NICK LEWIS

Internet2 NET+ Program

Manager, Security and Identity

AUGUST 20, 2015

INTERNET2

Founded

In **1996** by research universities ***to take self-responsibility for an advanced technology environment*** that would not otherwise exist—and exist when and how the research and education (R&E) community needs it

INTERNET2

INTERNET2

Goals

- Realize the ***power of collaborative scale*** to create capabilities no single institution could produce on its own

- Create ***advanced technology capabilities*** to extend leading edge scholarship and research

- ***Enable new generation of applications*** and core supporting infrastructure and technologies

- Achieve ***durable measure of control*** over the community's operating environment

- Transfer technology and experience to ***drive innovation and advance the global internet***
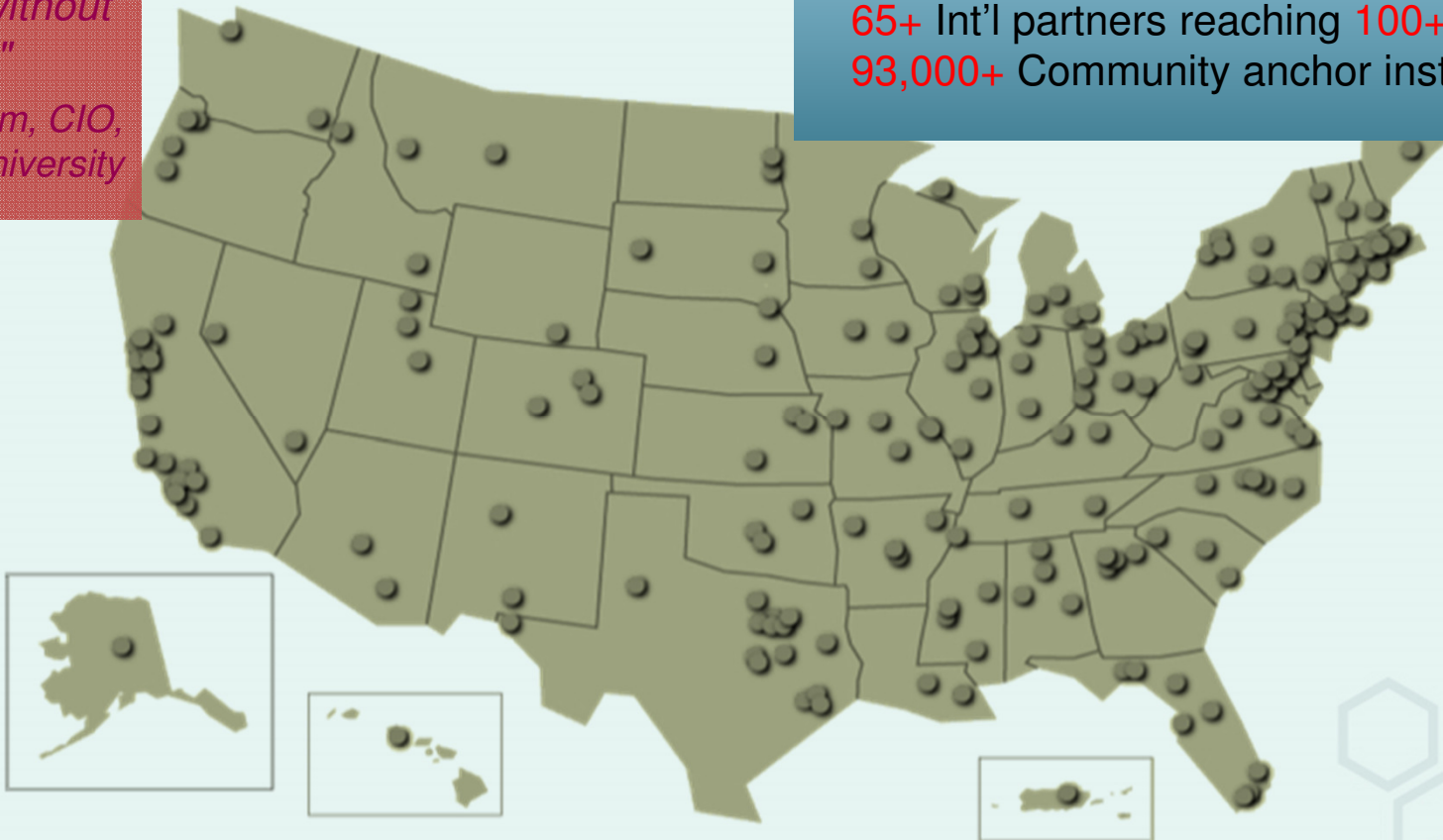
INTERNET2

INTERNET2

Community

- R&E member institutions, affiliates, agencies industry
- Rich and complex regional network community
- Global NREN community

Internet2 Members and Partners

"The idea of being able to collaborate with anybody, anywhere, without constraint…"

—Jim Bottum, CIO, Clemson University

285 Higher Education members
67 Affiliate members
42 R&E Network members
86 Industry members
65+ Int'l partners reaching 100+ Nations
93,000+ Community anchor institutions

INTERNET2

Internet2 100G Advanced Network

15,717 miles of newly acquired dark fiber

8.8 Tbps of optical capacity

2,400 miles partnered capacity with Zayo Communications in support of the Northern Tier region
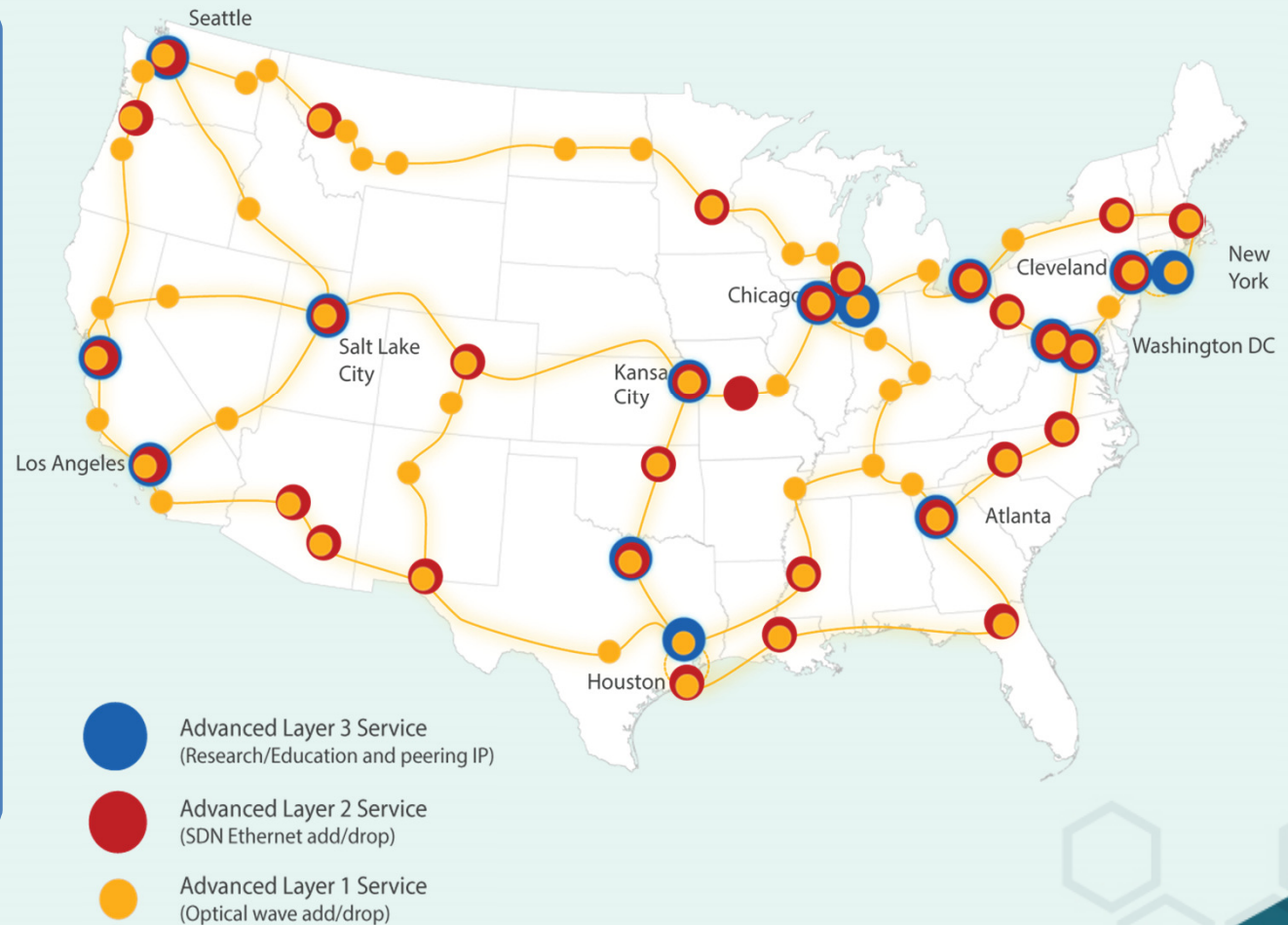
100 Gbps of hybrid Layer 2 and Layer 3 capacity

17 Juniper MX960 routers supporting Layer 3 service

31 Brocade and Juniper switches supporting Layer 2 service

49 custom colocation facilities

250+ amplification racks

300+ Ciena ActiveFlex 6500 network elements

Seattle
Salt Lake City
Chicago
Cleveland
New York
Washington DC
Kansas City
Los Angeles
Atlanta
Houston

● Advanced Layer 3 Service (Research/Education and peering IP)

● Advanced Layer 2 Service (SDN Ethernet add/drop)

● Advanced Layer 1 Service (Optical wave add/drop)

INTERNET 2

ADVANCING HIGHER EDUCATION

in the **Cloud**
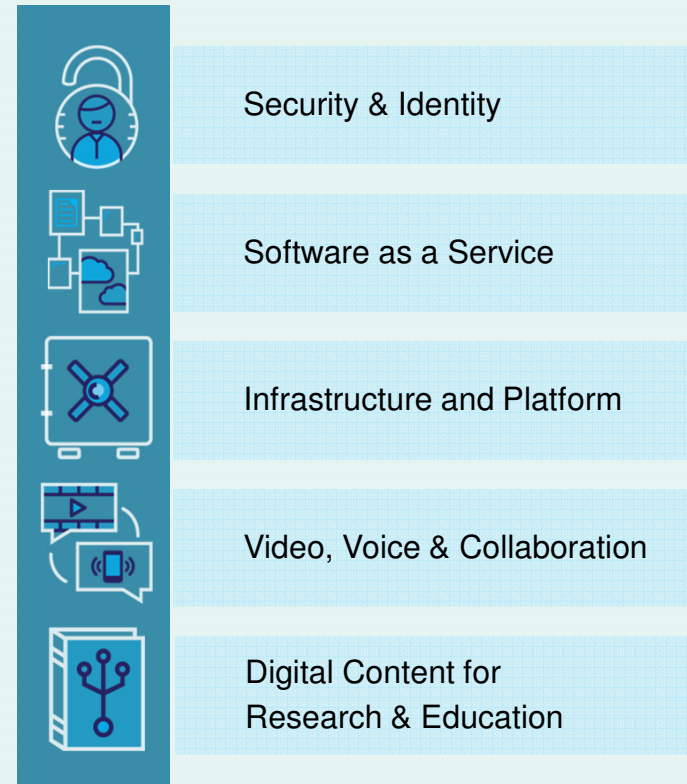
AND BEYOND

INTERNET 2®

NET+

INTERNET 2

What is Internet2 NET+ Cloud?

Internet2 NET+

Tailored Cloud service portfolios to:

- Enhance academic & research user mobility in the Cloud

- Accelerate trusted Cloud application deployment for the enterprise

- Ensure standards-based Cloud security, accessibility, reliability and performance with enterprise scalability

Security & Identity

Software as a Service

Infrastructure and Platform

Video, Voice & Collaboration

Digital Content for Research & Education

Enables trusted and responsive user mobility in the cloud, while delivering efficiencies to the enterprise.

INTERNET 2

Requirements of SPs

Identified Sponsor: CIO or other senior exec from a member institution

Membership in Internet2 and InCommon Federation

Adoption of InCommon -Shibboleth/SAML2.0 and Connection of services to the R&E Network

Completion of the Internet2 NET+ Cloud Control Matrix

Commitment to:

- A formal Service Validation with 5-7 member institutions

- Enterprise wide offerings and best pricing at community scale

- Establishing a service advisory board for each service offering

- Community business terms (Internet2 NET+ Business and Customer agreements)

- support the community's security, privacy, compliance and accessibility obligations

Willingness to work with the Internet2 community to customize services to meet the unique needs of education and research

INTERNET 2

Service Validation (SV)

Assessment of the service for inclusion in the catalogue, applying a consistent process, and determining how best to make it available at scale to the entire higher education community:

- SV Group is led by the Sponsoring institution and Internet2 and Includes:
    - Service Provider
    - Sponsoring University and 5-7 University Participants
- SV participants
    - Represent Peer Institutions and the Community
    - Apply consistent process to develop service for NET+ catalogue
    - Determine how to make it available at scale to the entire R&E community

Service Validation

Internet2 NET+ SECURITY & IDENTITY

- **Functional Assessment**
  - Review features and functionality
  - Tune service for research and education community

- **Technical Integration**
  - Network: determine optimal connection and optimize service to use the Internet2 R&E network
  - Identity: InCommon integration

- **Security and Compliance**
  - Security assessment: Cloud Controls Matrix
  - FERPA, HIPAA, privacy, data handling
  - Accessibility

- **Business**
  - Legal: customized agreement using NET+ community contract templates
  - Business model
  - Define pricing and value proposition

- **Deployment**
  - Documentation
  - Use cases
  - Support model

INTERNET2

SV: Business & Legal

Internet2 NET+   SECURITY & IDENTITY

- **Legal:** customized agreement using NET+ community contract templates

    MOU between Internet2 and Service Provider is signed in order to begin the Service Validation phase

    Business Agreement between Internet2 and Service Provider is negotiated during the Service Validation phase and reviewed and approved by university counsel

Business Model: customized approach to pricing that leverages community assets and captures aggregation to reduce costs to the Service Provider and provide savings and additional value to universities

Process and Deliverables: *Parties negotiate business agreements, enterprise customer agreements and any associated terms of use*

INTERNET2

SV: Technical Integration

Network: Integrate service with the Internet2 R&E network and optimize for enhanced delivery

> Test the network connection to create benchmarks

Identity: Review Service Provider's identity strategy and determine InCommon integration

> NET+ Identity Guidance for Services

Process and Deliverables: *Service Provider and participating universities assign technical team members on networking and identity; develop and review testing plans; and produce reference documents for service subscribers*

SV: Security & Compliance

Internet2 NET+

SECURITY &
IDENTITY

Security assessment: Customized version of the Cloud Controls Matrix (CCM) developed by the Cloud Security Alliance and SOC 2 Type 2 Report

https://cloudsecurityalliance.org/research/collaborate/#_internet2

Accessibility review and Roadmap commitment. WCAG 3C

Data handling: FERPA, HIPAA, privacy, data handling

Process and Deliverables: Service Provider completes Cloud Controls Matrix and/or SOC2 Type 2 Report for review by universities; campus accessibility engineers review service and communicate needs to Service Provider;

INTERNET2

Security and Identity Portfolio   Internet2 NET+

SECURITY &
IDENTITY

- Bring NET+ Principles to Security and Identity community

- Engage with the broadly defined higher education information security community in the portfolio development and adoption.

- Disrupt the status quo of how information security is integrated and executed at a campus to better manager the information security risk, improves privacy, and compliance on campuses.

- Make tools and services quickly available to campuses that aren't currently available because of cost, resources, or technical resources required.

INTERNET2

What is the SI Portfolio

access analysis anti-malware appliances application asset
authentication awareness bcdrp brokers cloud code config
control data device email encryption endpoint event grc identity incident
information intelligence loss
management mobile multifactor
network privacy protection response retention scanner
security source threat trust unified vulnerability web

What is *NOT* in SI Portfolio?

- TIER and InCommon

- Chief Cyberinfrastructure Security Officer – Paul Howell

- Other information security within Internet2

- Educause / HEISC

- REN-ISAC

- But, I am coordinating with these areas and the other NET+ Portfolios.

Focus on Security

Internet2 NET+

SECURITY & IDENTITY

- Updating "Recommended Process for the Use of the Cloud Controls Matrix (CCM) in the NET+ Program" and updating NET+ Cloud Controls Matrix

- Resource in NET+ program and in engaging with other PM's service providers

- Development of standalone "Security-as-a-Service" offerings

- Improve documentation and communication around how information security is handled in the NET+ program

  - Communications of existing security aspects of service validation. How NET+ can help from security perspective, etc

- Discussing sharing security evaluations among members, but not full service validation

INTERNET2

Sharing Security Evaluations

Internet2 NET+

SECURITY & IDENTITY

- Is this of interest of you and your teams?

- Would you actually use it?

- Would you be willing to share your assessments?

- Intent is not for "approval", but to help a campus save some time in managing their third party vendors and service providers

- Does this need to be more than just some metadata and a pointer to a report?

- Not a replacement for work HEISC is doing and not for NET+ service providers

- Trying for low maintenance, but high value

INTERNET 2

Security and Identity Portfolio

Internet2 NET+

SECURITY & IDENTITY

- A portfolio advisory board to be established
  - Campuses and regional networks, including an identity management representative to ensure close coordination with the identity community, InCommon and TIER.
- Work on a long-term strategy for 2016 and beyond on how to best support campus information security needs
- Short term, the portfolio has been jump-started via a request for new service providers or by a campus that sponsors a new tool via the NET+ service validation process.

Starting Engagement

- Outreach
    - Starting with a blog post reaching out to CIOs and CISOs
    - Development workshop at Tech Exchange
    - Discussed with Educause and REN-ISAC

- Who else should I reach out to engage? Where else?
- Mail list for discussion: netplus-sec-idm@internet2.edu

Service Provider Status

InCommon Certificate Service

Area: Security and Identity
Solution: Certificates
Provider: InCommon
Sponsor: InCommon

General Availability

Status

- Provides unlimited SSL, extended validation, client (personal), and code-signing certificates for one fixed annual fee, including all domains that you own or control.

Next Steps

Collaborate with InCommon

Duo Security

Area: Security and Identity
Solution: Multifactor Authentication
Provider: Duo Security
Sponsor: InCommon

OPEN

General Availability

Status
- Through its program with Internet2's InCommon, Duo Security offers an affordable pricing models for phone-based second-factor authentication: a site license for faculty/staff, faculty/staff/students, and campus associates.

Next Steps
Bring into NET+ Program
Forming Service Advisory Board

INTERNET 2

Splunk

Area: Infrastructure and Platform Services; Identity and Security

Solution: Machine data analysis

Provider: Splunk

Sponsor: Multiple Universities

General Availability

Status

- 3 year subscription term license at discounted rates
- 2nd Waterfall pricing threshold reached
- Community-developed software license agreement

Next Steps

Summer Advisory Board meeting. Discussing Splunk Cloud.

eduroam

Area: Security and Identity
Solution: Automated network access
Provider: Internet2

Early Adopter

Status

- Mature service (260+ participating institutions)
- Available to non-members
- About to enter General Availability

Next Steps

Complete service agreement, begin invoicing non-member institutions

eduroam

INTERNET2

DocuSign

Area: Security and Identity
Solution: Digital Signatures
Provider: DocuSign
Sponsors: Temple University

Early Adopter

Status

- DocuSign creates secure methods to capture electronic signatures and leverage paperless workflow
- Details on ordering and sign-up being worked out in early adopter

Next Steps

Sign-up service validation and early adopters
Service advisory board form

DocuSign

INTERNET 2

LastPass

Area: Security and Identity
Solution: Password Management
Provider: LastPass
Sponsors: Duke University

Early Adopter

Status

- Online/offline password manager
- Ready for Early Adopters

Next Steps

Webinar announcing service, start campus sign-ups and setup service advisory board

Adobe Document Cloud eSign

Area: Security and Identity
Solution: Digital Signatures
Provider: Adobe
Sponsors: Clemson University

Service Validation

Status

- Quickstart service validation
- Starting Service Validation

Next Steps

SV calls underway and sign business agreement.

Adobe Document Cloud

INTERNET 2

OpenDNS

Area: Security and Identity
Solution: Umbrella
Provider: OpenDNS (announced acquired by Cisco)
Sponsors: Clemson

Evaluation

Status

- OpenDNS is a leader

Next Steps

Working through quick start to get into NET+ program to complete SV within 2 years.

INTERNET2

CloudDLP Service Providers

Internet2 NET+

- We are currently talking or actively engaged with 9 different CloudDLP providers
  - Started with the Box DLP Webinar series
  - Adallom, CipherCloud, CloudLock, Code Green, Global Velocity, Netskope, Skyhigh, Symantec, and Websense
- All have the basics of scanning for sensitive data
- Forming working group to evaluate feature, functionality, etc
- Address privacy issues up front
  - How does a campus actually address the privacy aspects?

INTERNET2

CloudLock

Area: Security and Identity
Solution: Cloud DLP
Provider: CloudLock
Sponsors: Arizona State University

Service Validation

Status

- Quickstart service validation
- Working with CloudLock on service validation and identify additional campuses

Next Steps

-Start SV calls, define use cases, and get campuses involved. Start working on privacy discussions.
-Trying to get legal calls setup with campuses

INTERNET2

Skyhigh

Area: Security and Identity
Solution: Cloud DLP
Provider: Skyhigh
Sponsors: Brandeis University

Service Validation

Status

- Quickstart service validation
- Starting Service Validation

Next Steps

Start SV calls and sign business agreement. Start working though privacy discussions.

skyhigh

INTERNET 2

Netskope

Area: Security and Identity
Solution: Cloud DLP
Provider: Netskope
Sponsors: Open for sponsors

Evaluation

Status

- Netskope is a leader in cloud app analytics and policy enforcement. Netskope helps people safely use their favorite cloud apps so the business can move fast, with confidence.

Next Steps

Start SV calls and sign business agreement. Start working though privacy discussions.

INTERNET2

Fidelis Cybersecurity Solutions

Area: Security and Identity
Solution: Threat Intelligence
Provider: General Dynamics Fidelis
Cybersecurity Solutions
Sponsor: N/A

Inquiry

Status

- Working to understand NET+ model
- Seeking sponsor/service validators

Next Steps

Identify sponsor campus

Other Service Providers

- We have also talked with several potential service providers
  - Qualys
  - HP Fortify on Demand
  - Akamai for DDoS service
  - Black Lotus (acquired by Level 3) for DDoS service
  - AlienVault for SIEM service
- Any interest in these types of tools
  - Web app security scanners – Whitehat Security?
  - Endpoint security – Bit9+Carbon Black?
  - Mobile Device Management – Airwatch?
  - ITGRC – Service Now (in SV), RSAM, etc?
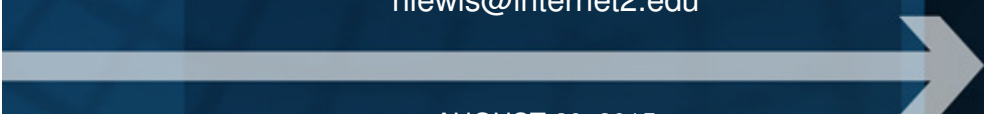 - Threat intelligence – Fidelis Cybersecurity?

INTERNET 2

NICK LEWIS

nlewis@internet2.edu

AUGUST 20, 2015

INTERNET2 NET+ SECURITY AND IDENTITY PORTFOLIO