



IT SECURITY

RANDY MARCHANY

Virginia Tech IT Security Office and Lab
marchany@vt.edu



THE UNIVERSITY IT SECURITY MODEL IS SIMILAR TO A MUSEUM



Photo by Pueri Jason Scott, https://commons.wikimedia.org/wiki/File:Mona_lisa_crowd.jpg. Licensed under the [Creative Commons Attribution-Share Alike 3.0 Unported](#) license.

- **Control Access:** we have limited but **free-flowing** access points with additional protection around high-risk assets.
- **Pervasive Outbound Monitoring:** We invest in monitoring and quick response to threats to protect users, data, and systems. We assume hostiles are inside already.
- **Active Response:** rapid isolation of compromised machines, data
- **Recovery Measures:** backups, cybersecurity insurance, data trackers

We have long followed what is now called the “zero-trust network” model. Each computer should be appropriately secured. We focus on protecting data, regardless of where they physically reside.

VIRGINIA TECH BUSINESS PROCESS IT SECURITY MODELS



Administrative

- Process that runs the university
- Security: **CORPORATE**



Academic / Instructional

- Process that supports teaching/learning
- Security: **ISP***

*Internet Service Provider



Research

- Process that supports VT Research
- Security: **HYBRID**

Challenge: create an overall security architecture that blends these 3 business process IT security requirements

SHARED RESPONSIBILITY MODEL



Responsibility is
bottom-up.

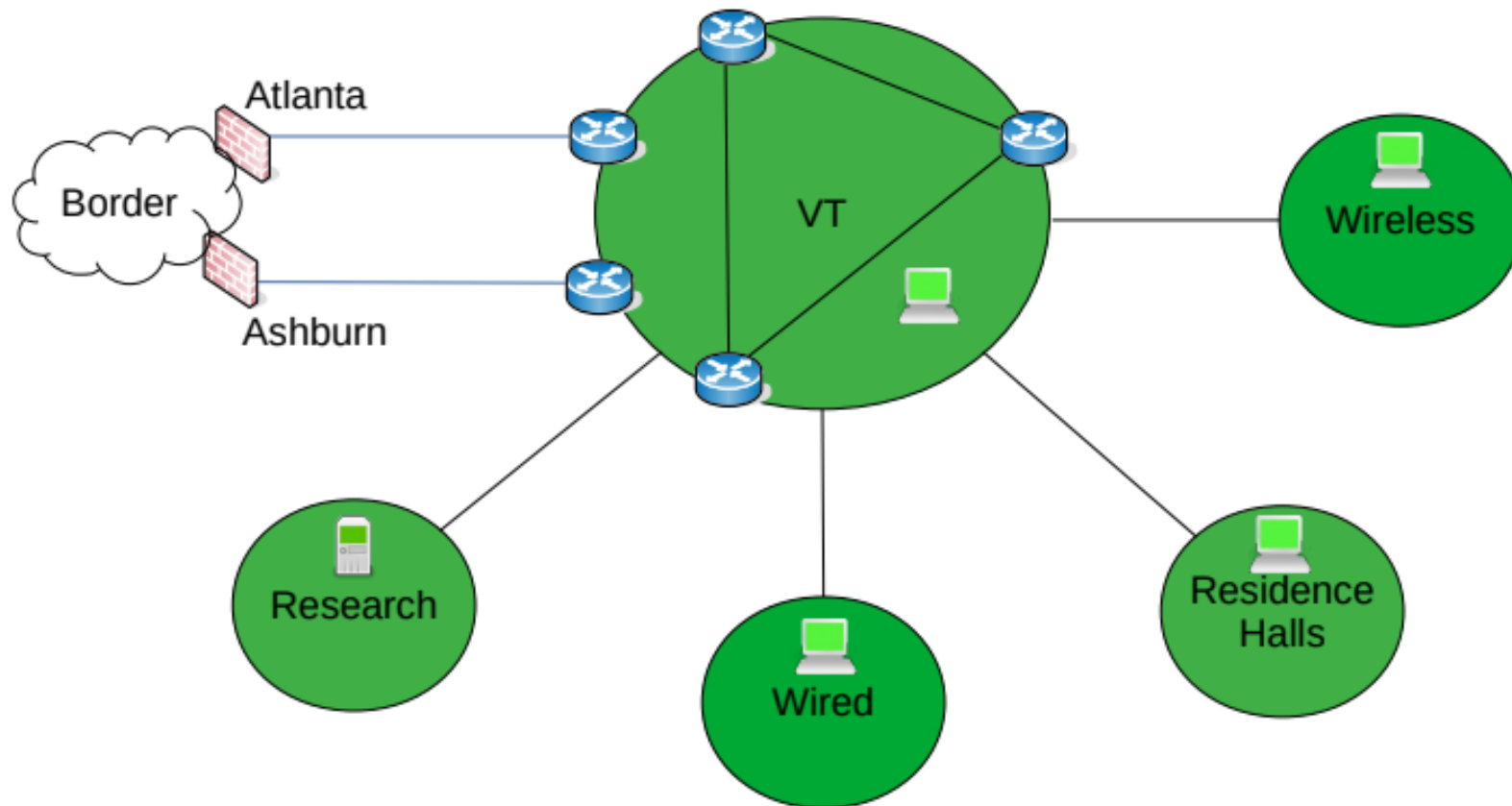
Enforcement is
top-down.

All security starts
local.

- All VT policies for IT security apply to the individual regardless whether they're faculty, staff, student, alumni, guest, etc.
- Individuals are responsible for all actions from their user IDs or devices they own or manage on behalf of the university
- Departments/colleges work with ITSO, OARC to ensure policy compliance
- Enforcement of IT security policies delegated to the VPIT/CIO; further delegated to the ITSO

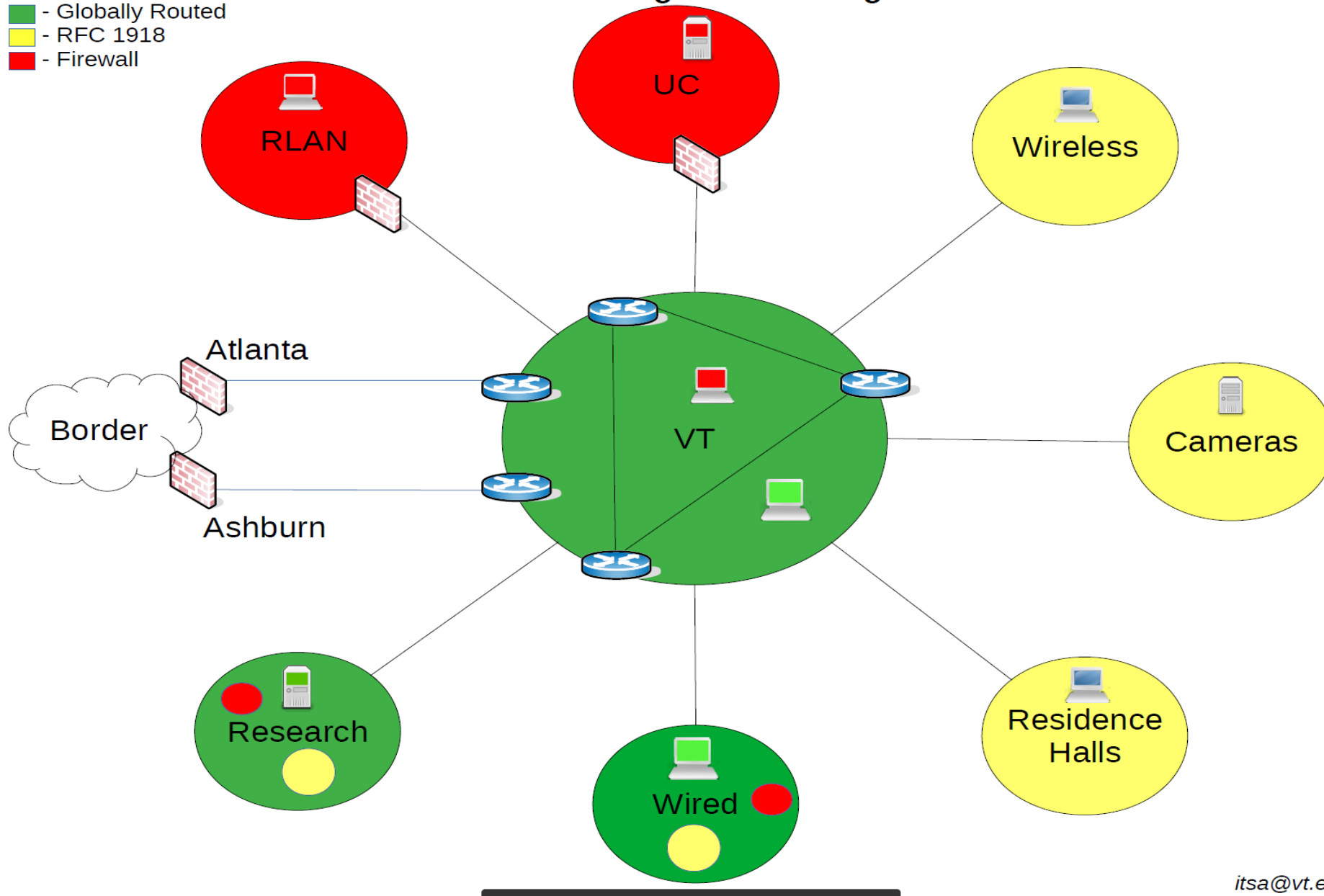
Past - Network Segments at Virginia Tech

■ - Globally Routed



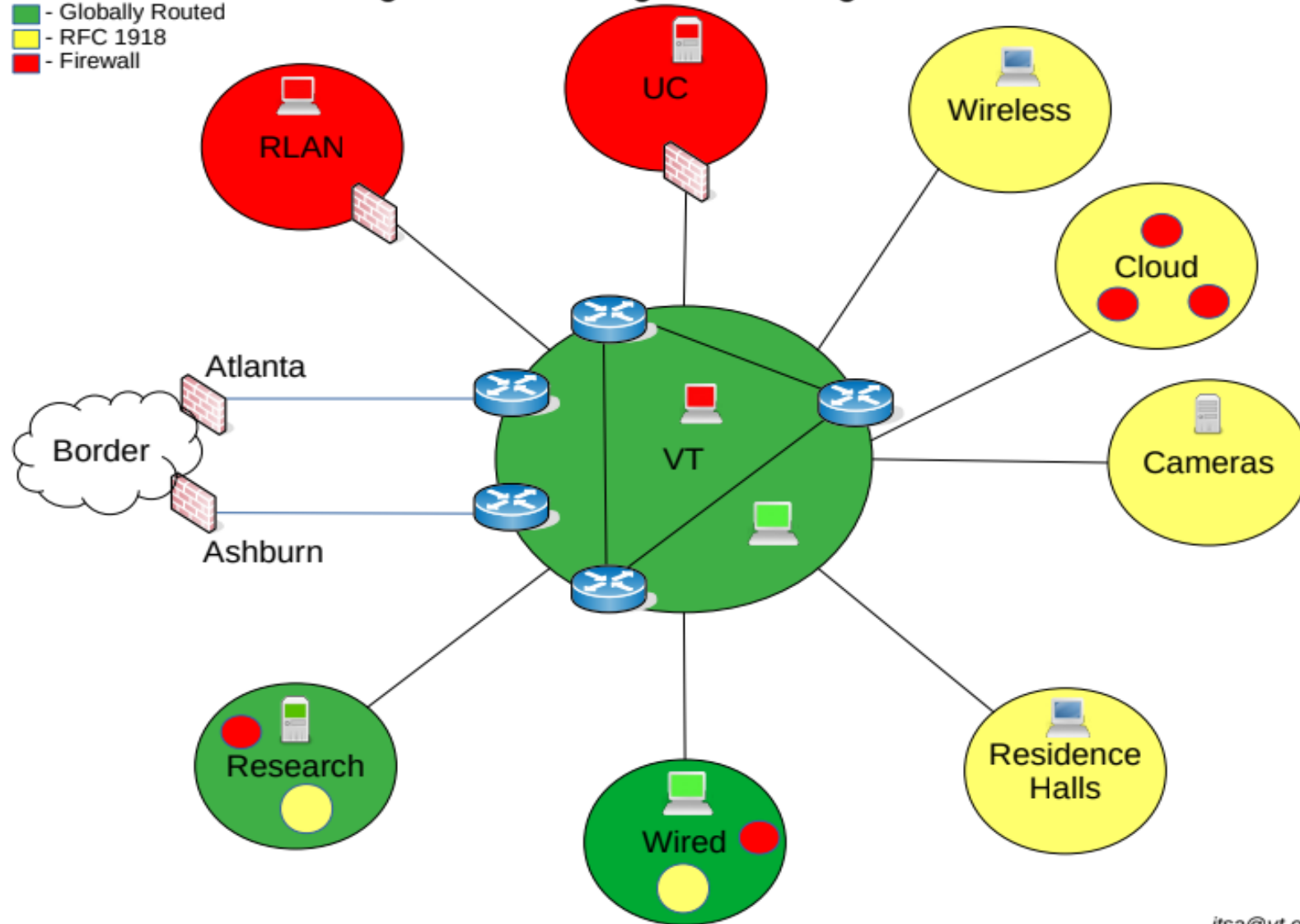
Current - Network Segments at Virginia Tech

- - Globally Routed
- - RFC 1918
- - Firewall



Target - Network Segments at Virginia Tech

- - Globally Routed
- - RFC 1918
- - Firewall



IT Security Architecture

Local Addressing – 172.x.x.x

- block unsolicited inbound
- Can be used for printers and other devices
 - accessible from outside via VPN

RLAN – with inline Palo Alto FW

Wireless NAT

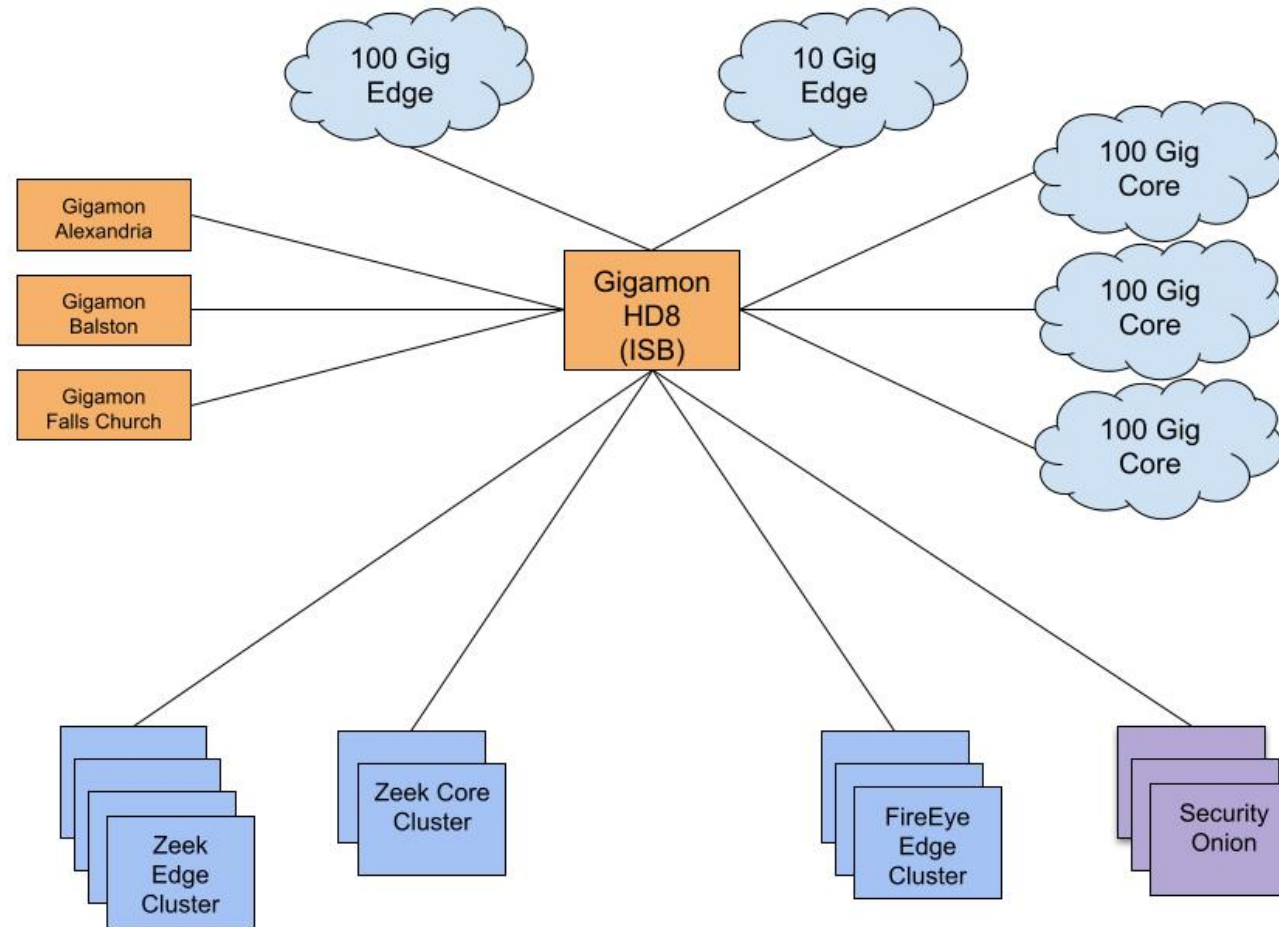
Microsoft ATP

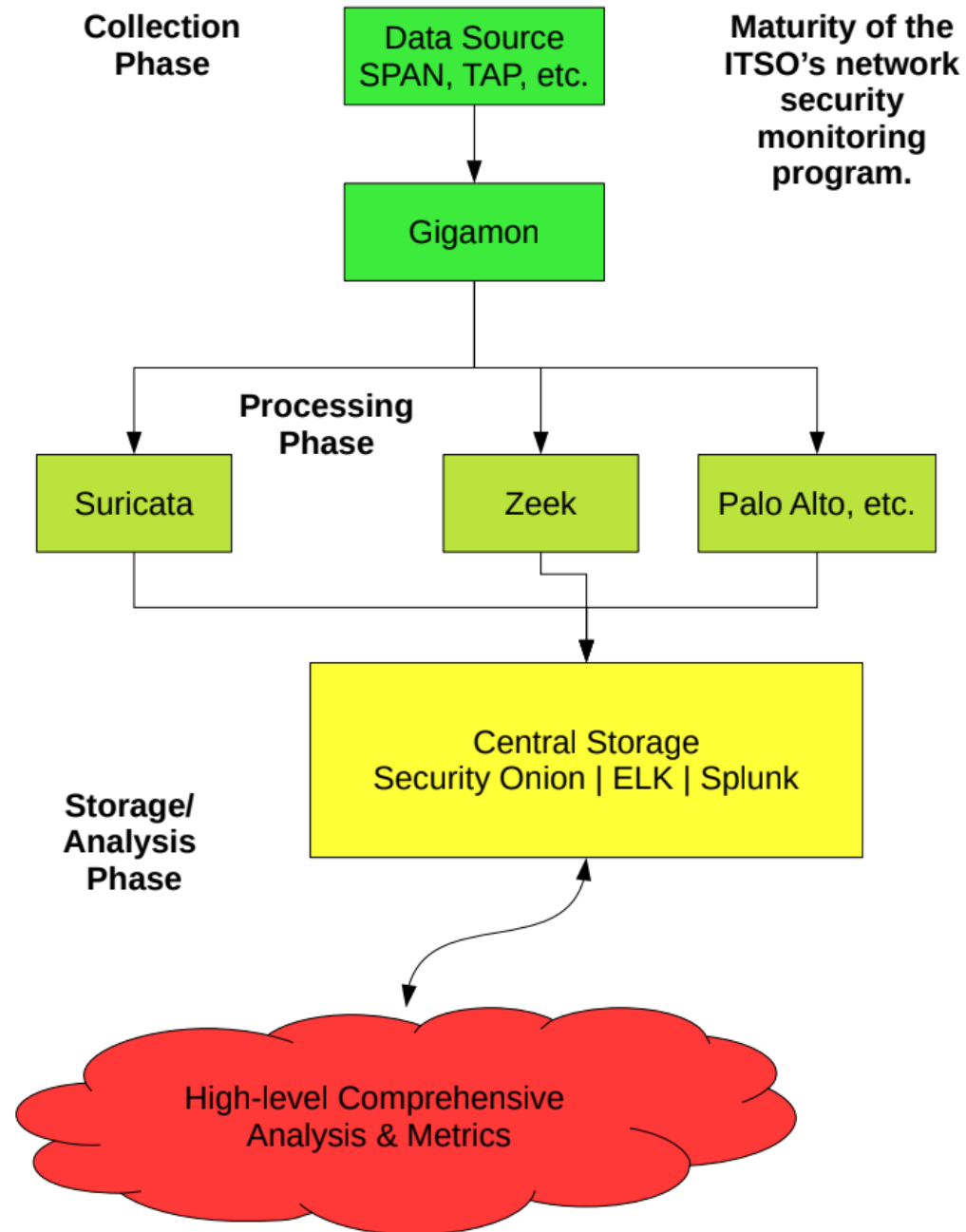
Host Based FW

Aveya VOIP segment with inline FW

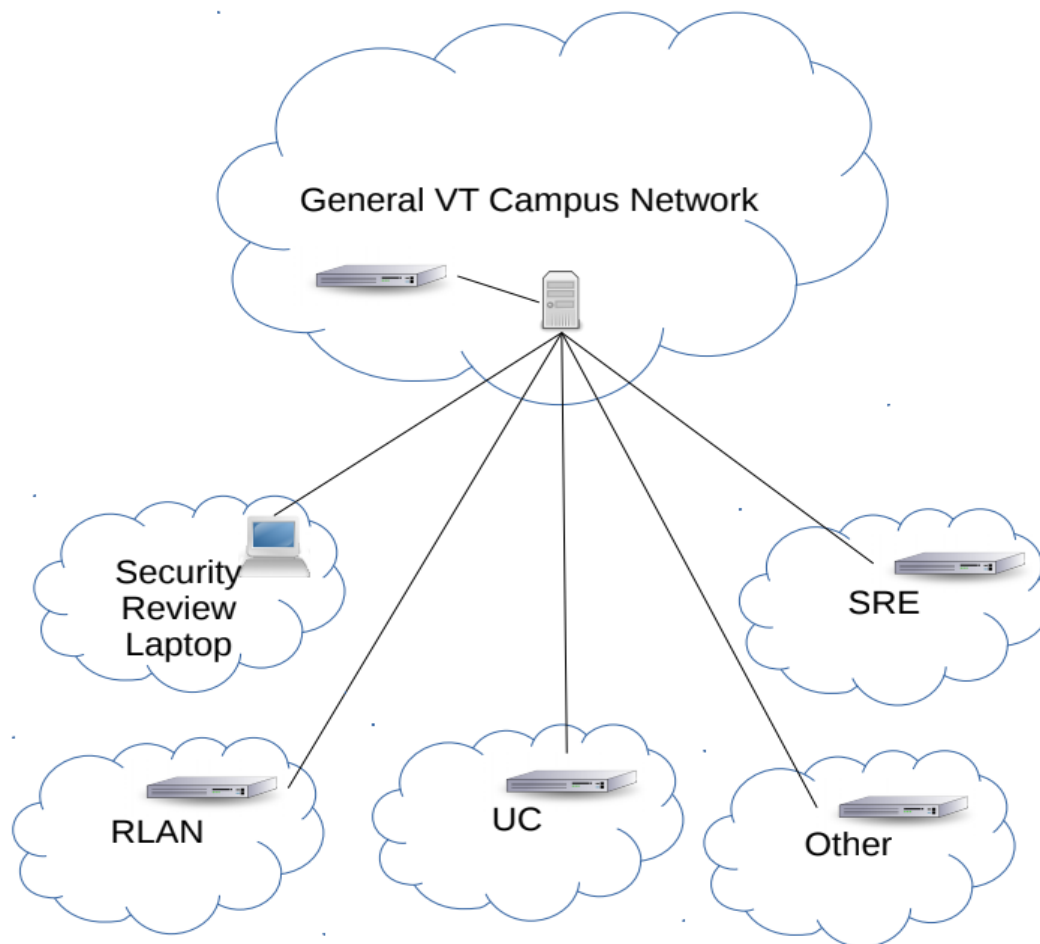
9 Main segments – Wired, Wireless, VOIP, Network MGT, RLAN, ICS, Surveillance Camera, VTCRI, 172.x.x.x

ITSO IDS/IPS Architecture





Planned - Virginia Tech Vulnerability Scanning Architecture



There will be five scan engines. Each network segment will have a dedicated vulnerability scan engine. There will be a floating laptop with a software-based scan engine for security reviews. There will be a central management console for reporting and aggregating scan results. There will be an API on the management console.

Total IP addresses to scan will be 5,000 across all segments.

ISORA Risk Management Tool



RISK OVERVIEW

Attacker goals over the past 30 years fall into three basic categories:

- **Data Theft and/or Disclosure**
- **Data Destruction**
- **Attacking other sites using organization's assets**

Increasing regulatory and compliance requirements require significant resources and expertise to manage and mitigate. ISORA helps departments categorize their risk and mitigation strategies.

RISK EXAMPLES

- **Cyber attacks originating from University assets**
- **Cyber attacks leading to deliberate exposure or loss of high or medium risk data**
- **Accidental exposure of high or medium risk data**

Increased compliance and regulatory requirements and heightened regulatory scrutiny for data and IT systems

Loss of institutional reputation and trust

MITIGATION EXAMPLES

- **Continuous network monitoring**
- **IT security reviews; vulnerability scans; internal penetration testing; digital forensic services**
- **Security awareness training**
- **Computing enclaves to ensure compliance**
- **Minimum security standards, Center for Internet Security "Critical Controls v8.0"**
- **Enhanced authentication (MFA) Central Logging Service (CLS)**
- **Embedding IT security practices in University business processes**

AUDIT ISSUES & MITIGATIONS

ISSUES

- **Not scanning for high risk data such as SSN, Driver's License numbers, passport numbers, bank and debit account numbers on a regular basis**
- Lack of consistent software patching
- Lack of whole disk encryption
- Inconsistent logging practices
- No IT risk assessments in the past 3 years
- Unapproved software on endpoints
- Endpoint administrative privileges not restricted

MITIGATIONS

- MINIMUM security standards for endpoint, servers and applications
- Departments running high risk scanning tools on a regular basis
- DoIT central endpoint management tools coming online
- Department action plans to address OARC findings
- Training and awareness programs for general users and for users who need endpoint administrative privileges
- ITSO Risk Assessment team working with departments to complete their IT risk assessment using ISORA
- Improving efficiency of software procurement security reviews



ADDITIONAL MITIGATIONS



- DNS “Firewall” intercepts and blocks callbacks to known bad sites
- Streamlined IT Risk Assessment process (ISORA) for departments
- Track CSC Security Controls progress
- Interactive Phishing Awareness Training available to all departments
- Increased security awareness campaigns
- Policies, standards, skills training
 - VT IT Policies & Standards: <https://it.vt.edu/resources/policies.html>
- Emphasis on data analytics

INCIDENT STATISTICS

2018-2020

- **68** POTENTIAL PII EXPOSURES
 - **3** “NEAR MISS” INCIDENTS
 - Verified PII, high risk data did **NOT** leave VT
 - **1** ACTUAL PII EXPOSURE INCIDENT
 - **36** records with PII exposed and notifications sent
- **21** RANSOMWARE INCIDENTS
 - **1** successful enterprise wide ransomware attack involving institutional data. Local security software blocked the attack.
 - **3** successful ransomware attacks involving individual data. Data restored from backups.

Kaseya Ransomware Attack against Virginia Tech

- Three VSA servers running on campus in three departments.
- One of them had the administrative interface available to the Internet and was compromised.
- Six additional departments actively used this VSA for management.
- Machines impacted.
 - **Servers: 111**
 - **Endpoints: 805**
- Encryption followed all shared drives and drive synchronization with Google Drive and Microsoft OneDrive.
- Multiple file servers were encrypted by those shared drives

Things that worked well – Kaseya Attack

- The overall cyber incident response and CIRT activation worked as designed.
- Communication between departments was clear and concise. Information sharing was appropriate and timely.
- The initial departmental response to the attack was quick and effective.
- Daily update meetings during the initial phase of the incident response were critical to a successful response.
- Division of IT units beyond the ITSO, responded quickly to requests for portal blocks, storage adjustments, physical hardware, and staff to help departments with response and recovery.
- Network forensics expediently verified that no data was sent off campus.

Things that didn't work well – Kaseya Attack

- Administrative console access to Kaseya was open to the internet.
 - Access to these consoles should be limited and monitored.
- The list of University business contacts used by the CIRT was outdated.
 - Updating contact information is important, missed some critical areas with initial contact.
- High risk data inventories were incomplete and outdated.
 - Scans to ID high risk data should be done regularly especially on file shares.
- The prioritization of data and system recovery workflow could be improved.
 - This added critical time to identify high priority data especially when we were considering “pay the ransom” option.
- Changes to Department of Education requirements weren't well understood.
 - There are now reporting and tracking requirements for incidents.
 - 72 hour window to report breach from the time of the attack.

Things that didn't work well – Kaseya Attack

- Out of band information about machines managed by Kaseya was not available and some machines were no longer actively managed but still retained the client software.
 - This caused trouble identifying machines that were impacted some discovered weeks later.
- Most areas did not have sufficient storage resources to backup, reinstall and recover their systems.
 - Needed to borrow systems and storage from other areas delaying recovery efforts
- Physical forensics were negatively impacted by large drive sizes and lack of sufficient duplication equipment
 - ITSO didn't have the resources to take images. Either need to increase this or have a standing relationship with a company that can do this.


Recommendations

- The ITSO should document as a best practice that systems and services that have elevated privileges limit administrator access to, at a minimum, only on-campus addresses.
- These systems which include things like Big Fix, inTune, Jamf, Kaseya, Nanite should have security reviews regularly to ensure they follow the best practices.
- They should have additional logging and monitoring including logging to a central service.
- Business continuity and backup plans should include the resources necessary to rebuild and restore systems.

Kaseya Attack - Other items of interest

- Distributed IT groups that provide services to other departments needs to be understood and appropriately scoped.
- Enterprise level backup needs to be reviewed and moved in a consistent direction.
- There are an insufficient number of IT professionals to take on many of the preventative measures to more completely protect against cyber threats and provide timely recovery when events occur.
- **It is not over. Departments are still scanning file shares and identifying data.**

ITSO Services



SECURITY

QUICKLINKS

ABOUT

INCIDENT RESPONSE

SOFTWARE

SERVICES

RESOURCES AND INFORMATION

MORE

IT Security Office

Services

Rights Management Services / Microsoft Information Protection

Vulnerability Scanning

IT Security Reviews

Web Application Scanning

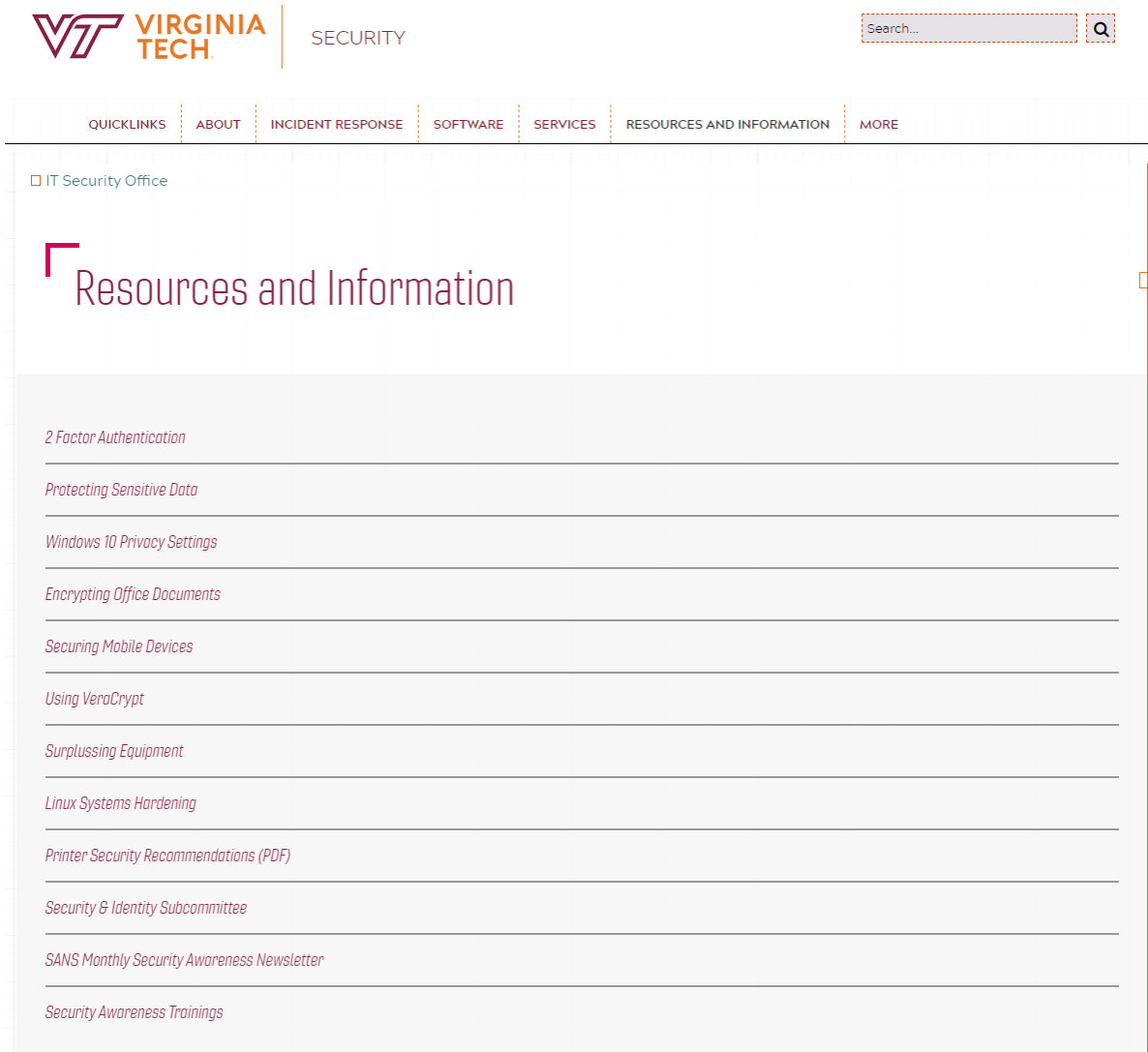
Awareness Training

Application Reviews

Big Fix

RLAN

ITSO Resources and Information



TOP 3 CHALLENGES



- In-house, vendor, distributed computing risks
 - Risk of data exposure
 - Vendor questionnaires allow risk assessment
 - Staff shortages to evaluate these issues



- User cybersecurity awareness
 - User training and awareness
 - Technical training for IT staff
 - Need to “see something, say something”



- Software patching
 - Unified Endpoint Management program

COMPLIANT



SECURE

