



VCU

# Zscaler

Faculty Senate

*Jesse Castellani - Security Architect*  
*Dan Han - CISO*

# Agenda

---

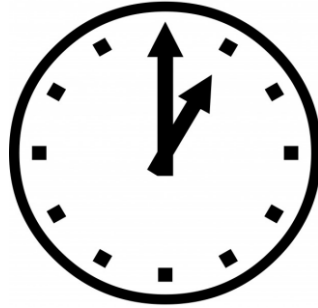
- Goals and Challenges
- Zscaler Overview
- HTTP Overview
- FAQ / Q&A

# Business Aspirations

---



Anywhere



Anytime



Ease



Secure

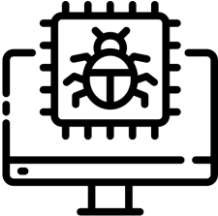
---

# Security Challenges

74% ↑



358% ↑



Source: Sobers, Rob. "166 Cybersecurity Statistics and Trends [Updated 2022]" Varonis. Varonis. August 3, 2022. <https://www.varonis.com/blog/cybersecurity-statistics>



- VPN 2.0
- Security Features:
  - Firewall as a Service
  - Secure Web Gateway
  - Malware detonation chamber
  - Phishing site detection and prevention
  - Intrusion detection and prevention
  - Reverse Proxy Based always-on remote access
  - Device posture management
  - Application based access control
- Zscaler Agent Client (ZCC)
- ZScaler Internet Access and ZScaler Private Access

# Zscaler Client Connector (ZCC)

## macOS



## Windows



The screenshot shows the Zscaler Client Connector application window. The title bar reads "Zscaler Client Connector". The interface features a blue header with the Zscaler logo and a "Log Out" button. The main content area is divided into two columns. The left column contains several status indicators: "Private Access" (with a lock icon), "Internet Security" (with a shield icon), "Digital Experience" (with a person icon), "Notifications" (with an exclamation mark icon), and "More" (with a three-dot icon). The right column displays connectivity and statistics information.

Connectivity	
Username	jacastellani@vcu.edu
Service Status	ON    TURN OFF
Network Type	Off-Trusted Network
Authentication Status	Authenticated
Broker	136.226.73.252
Client	192.168.0.181
Time Connected	Thu, Nov 17 2022 06:13:00 AM
Protocol	TLS

Statistics	
Total Packets Sent	2.15 MB
Total Packets Received	594.47 MB



## Internet Access

---

Consistent security policy for network and applications

Warning of potentially malicious and dangerous sites

File inspection and malware detonation

DLP capabilities

Risk-based classification of third party apps



## Private Access

---

Always-on access to internal university resources

Reverse-proxy exposes access to application

Device posture check

Application health monitoring

Pre-authentication connection to internal resources

Risk-based access control

# Zscaler - Warning Example



**⚠ Are you sure you want to visit this site?**

You tried to visit: <http://pastebin.com/>

Request method cautioned for category **Anonymous Paste Sites**

Proceeding to visit the site may be dangerous and/or may violate VCU's Computer and Network Resource Use policy. Press the "Continue" button to access the site anyway or press the "Back" button on your browser to go back

[Continue](#)

[See our internet use policy.](#)

Need help? Contact our support team at +1 (804) 828 - 2227, [itsupport@vcu.edu](mailto:itsupport@vcu.edu)

C03



# Zscaler - Block Example



⊘ We found a security threat.

The site you are trying to visit is not permitted. If you believe this site is blocked in error, then please contact the VCU IT Support Center at (804) 828-2227 or [itsupport@vcu.edu](mailto:itsupport@vcu.edu)

You tried to visit: <http://example.com>

Threat found: **Virus**

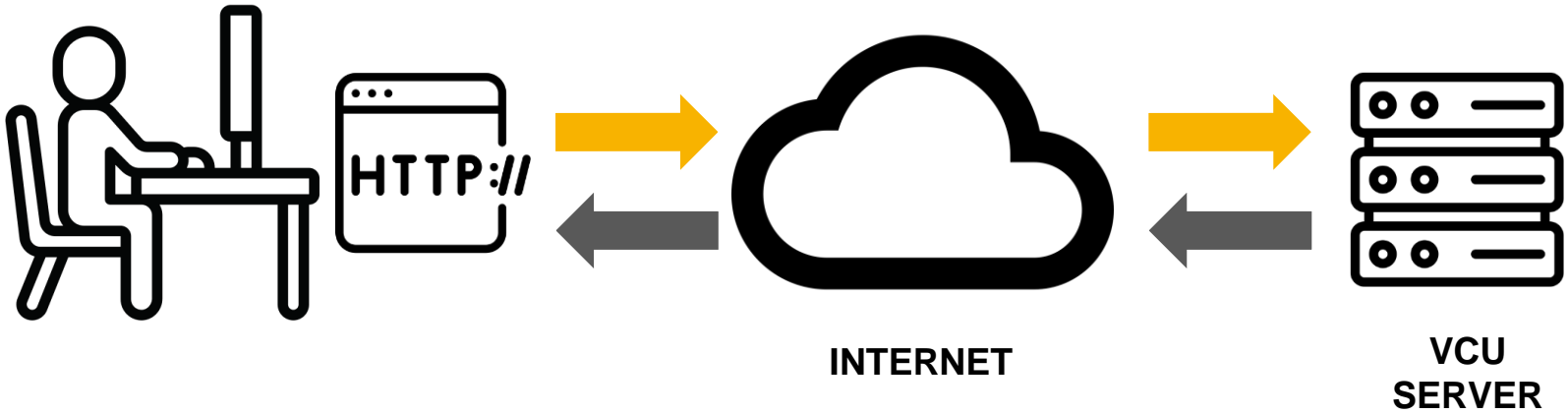
[Click to request security review.](#)

[See our Internet use policy.](#)



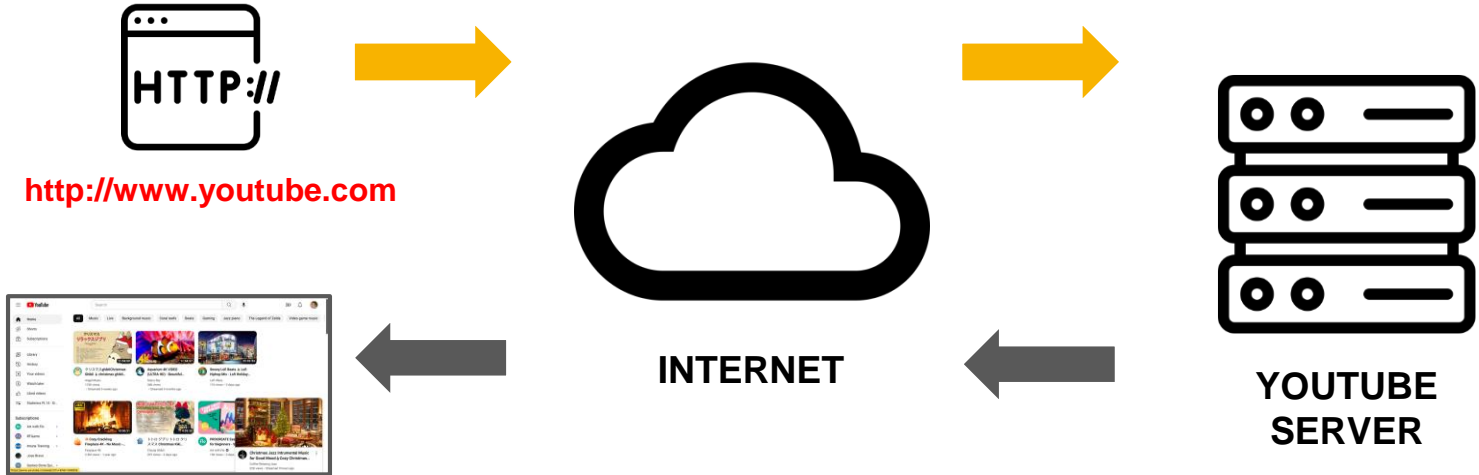
# How Does Zscaler Work?

# HTTP Overview

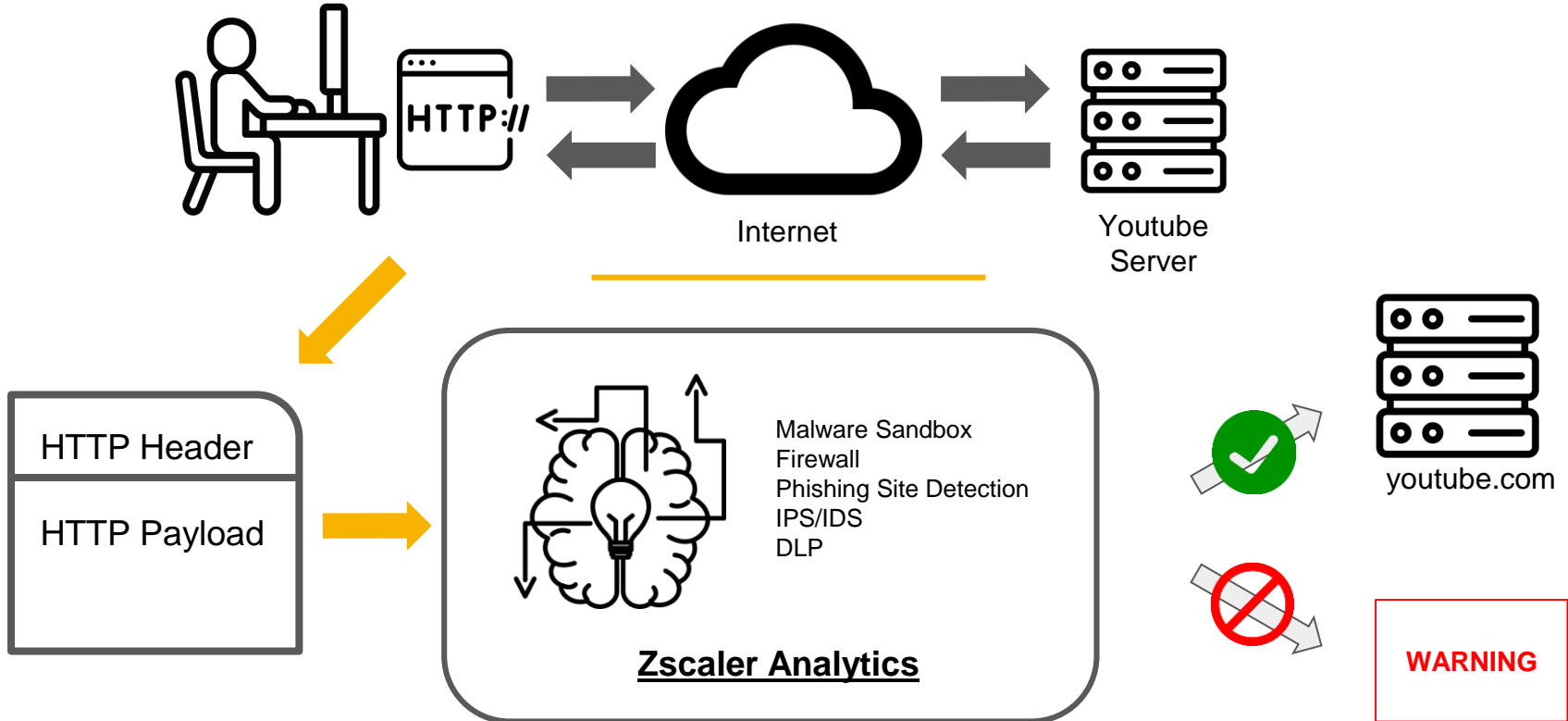


# HTTP (Hyper-Text Transfer Protocol)

- How our computers request and load **websites**



# How It Works with Zscaler



# Comparison

---



Access VCU Applications?



---

Continual Access?



---

Detect Malware/Phishing?



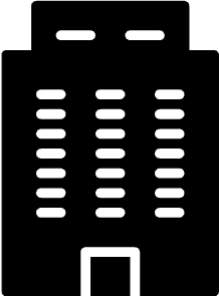
---

Protect from Harmful Traffic?



# Accomplishes

---



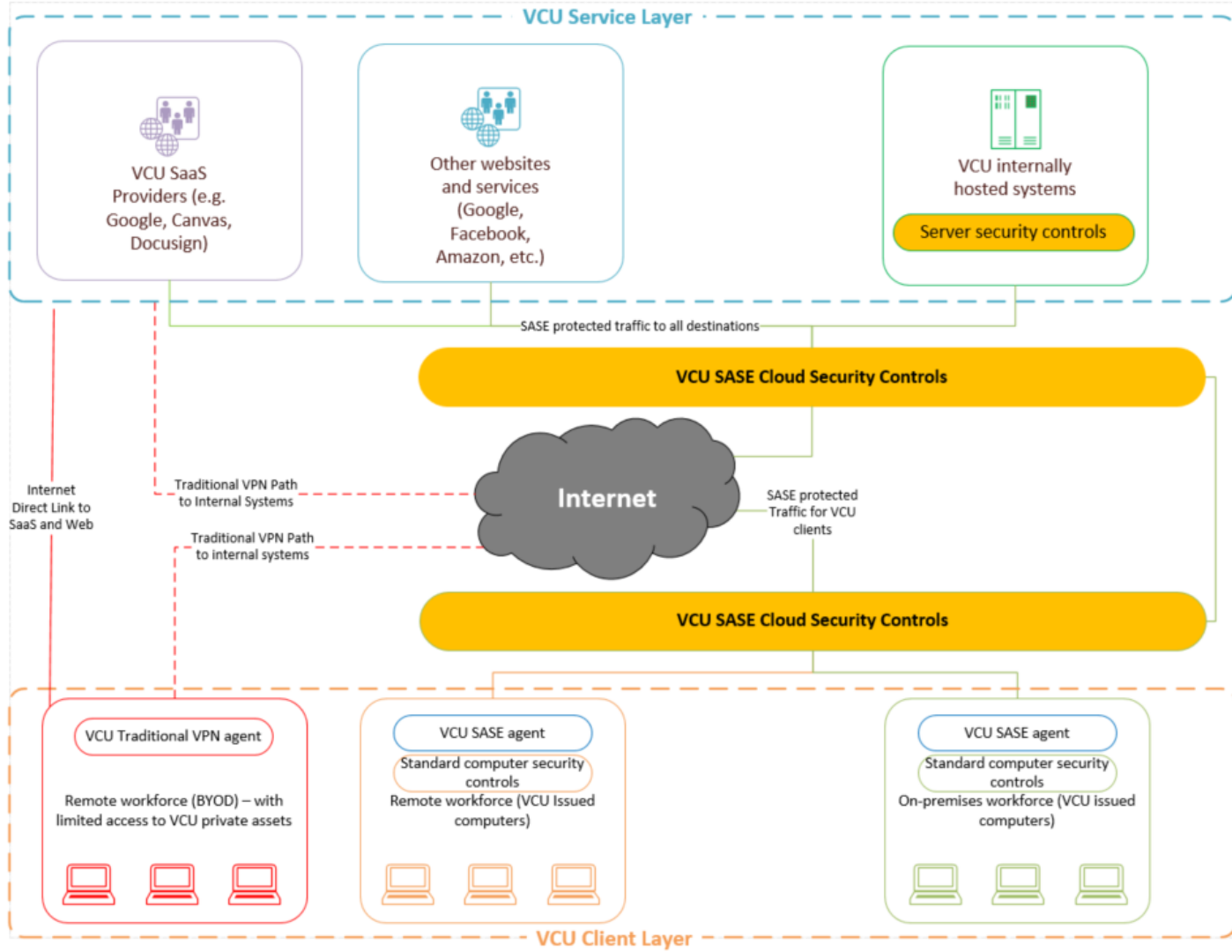
&



=



# Future VCU Security Model



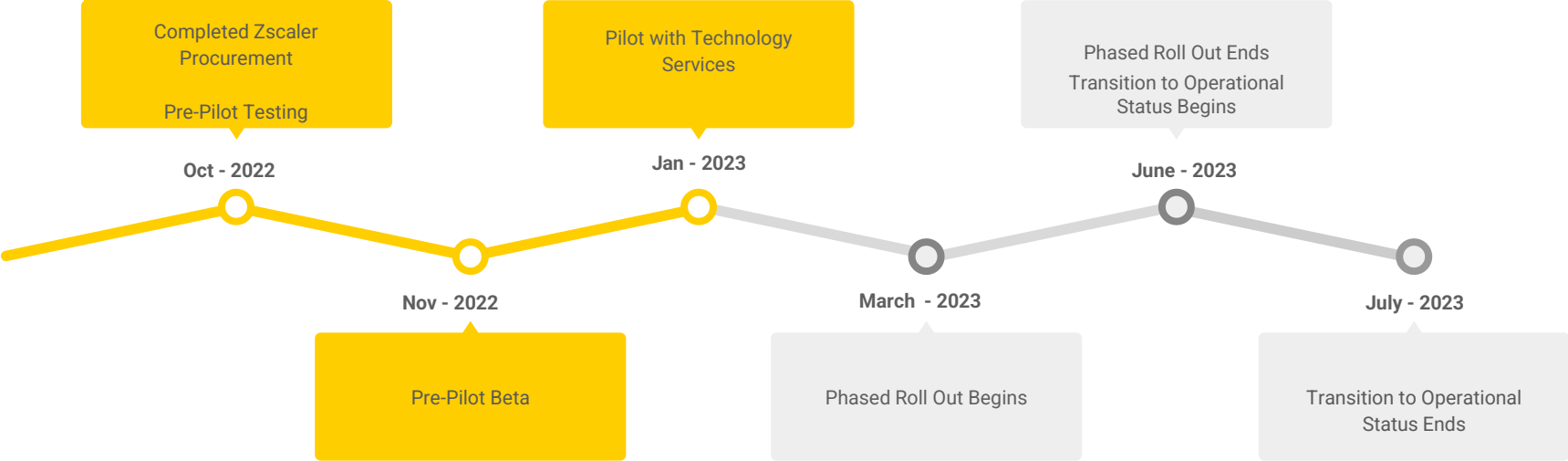


# Roll-Out Plan



- Currently working with the vendor in designing and implementing the solution in our environment.
- Engaging all schools, colleges, and units in helping us test both the Internet protection and private access aspects.
- Need to build out access rules for private assets (e.g., SSH to a server, printing system, other unique access to assets).

# Tentative Project Timeline



# Zscaler FAQ:

---

## **Who is it intended for?**

*VCU Employees, Student Workers, Graduate Assistants, and Affiliates*

## **What devices can install the Zscaler Application (ZCC)?**

*VCU Managed Devices*

## **What are the limitations of Zscaler?**

*Server initiated connections through ZPA (e.g. Wake-on-lan) are not possible at this time.*

## **What will students use?**

*Cisco AnyConnect VPN*

# Zscaler FAQ Con't

---

## **Will Zscaler replace Cisco Anyconnect?**

*No. Although in the future, sensitive applications would be limited to Zscaler.*

## **Can I use Zscaler and Cisco Anyconnect at the same time?**

*Yes. There are some limitations when using ZPA and Cisco Anyconnect.*

## **Do I have to reconnect to Zscaler everyday?**

*No.*

## **What can VCU see when I use Zscaler?**

*While using Zscaler, VCU has access to logs and other metadata for network traffic while using Zscaler.*

Q&A

