Zscaler

Faculty Senate

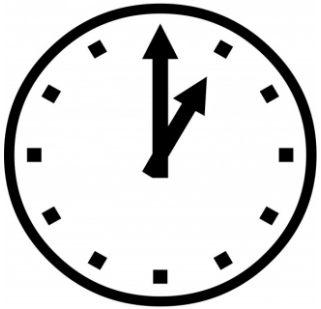
Jesse Castellani - Security Architect
Dan Han - CISO

Agenda

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

Business Aspirations

Anywhere



Anytime

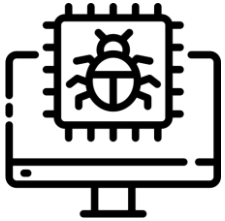
Ease

Secure

Security Challenges

74% ↑

358% ↑



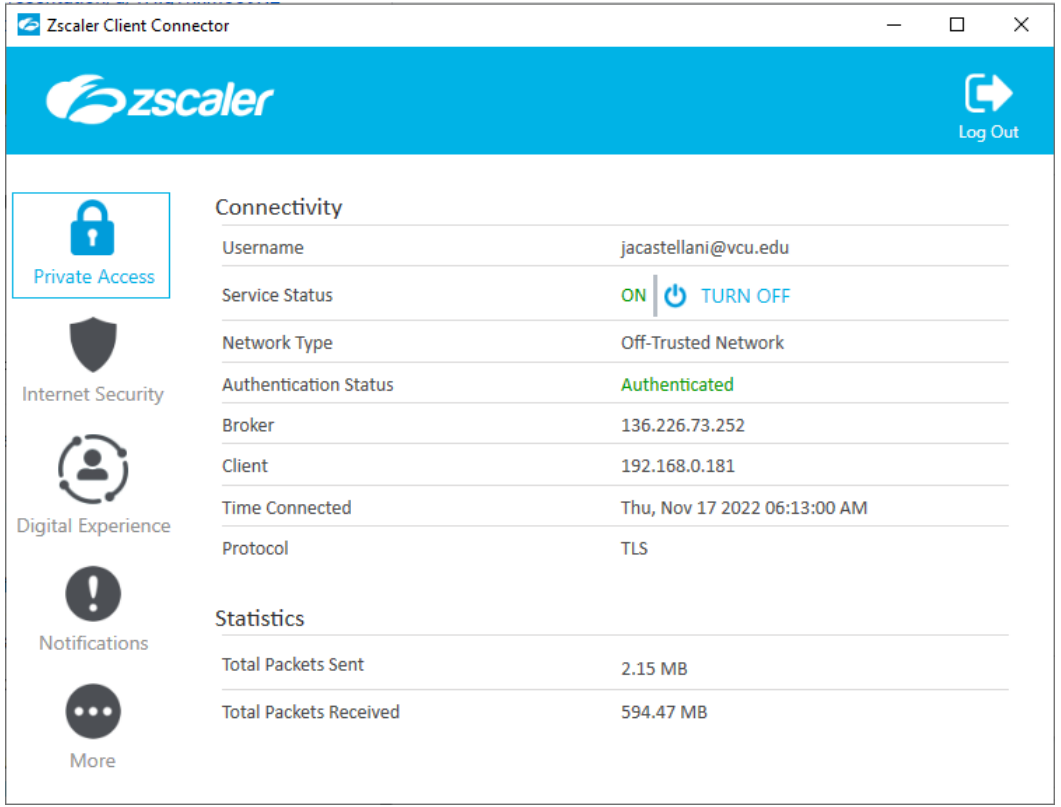
Source: Sobers, Rob. “166 Cybersecurity Statistics and Trends [Updated 2022].” Varonis, Varonis, August 3, 2022. https://www.varonis.com/blog/cybersecurity-statistics

- 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



Internet Access

Consistent security policy for network and applications

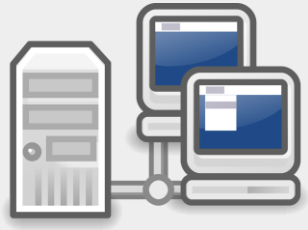
Warning of potentially malicious and dangerous sites

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

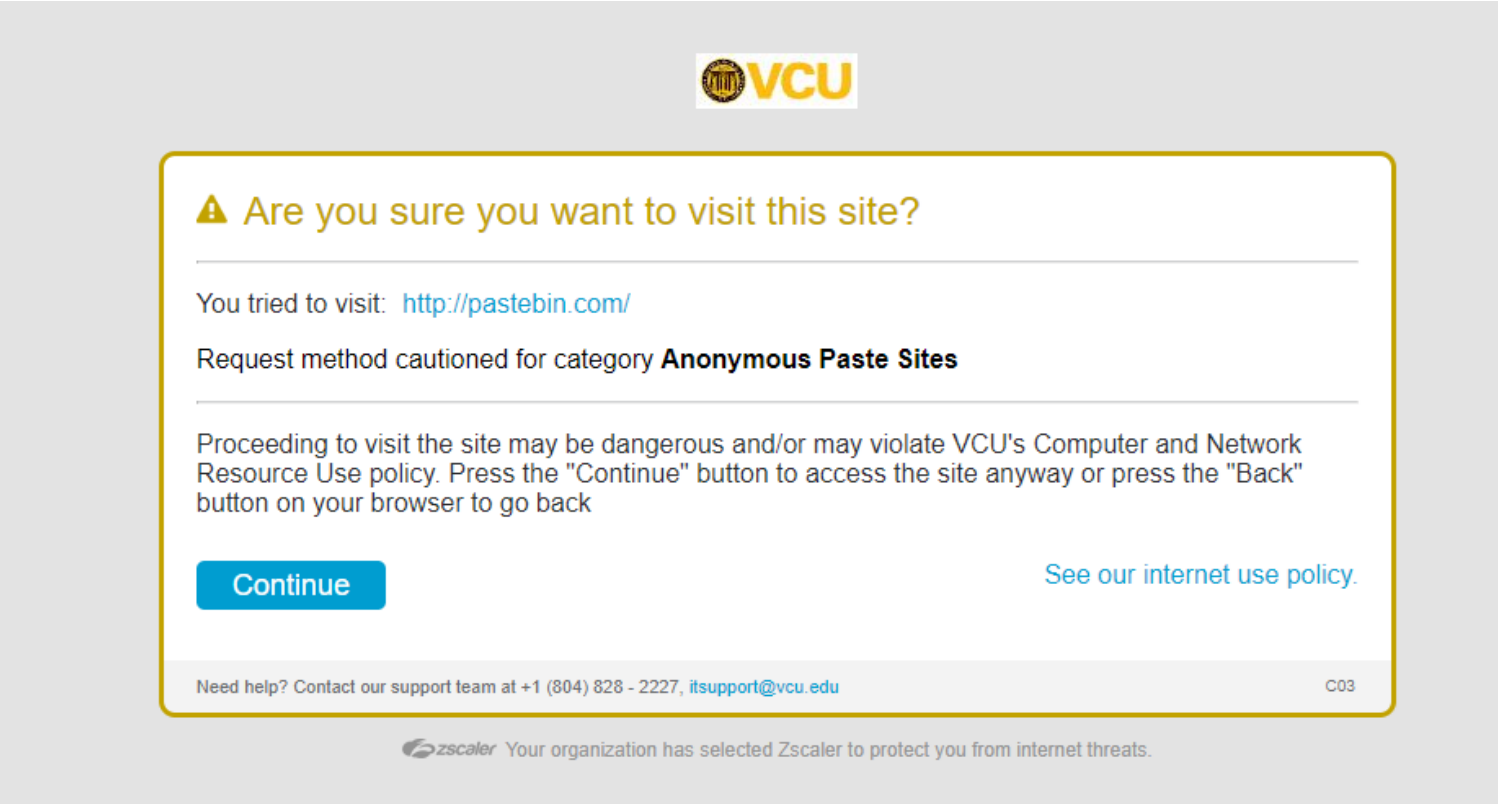
Device posture check

Application health monitoring

Pre-authentication connection to internal resources

Risk-based access control

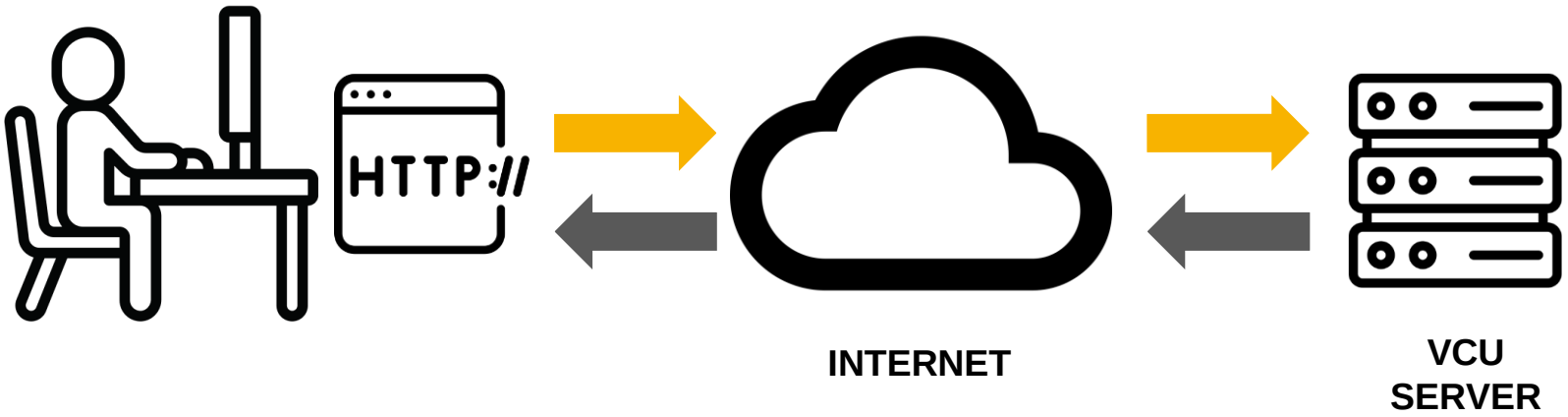
Zscaler - Warning Example



Zscaler - Block Example

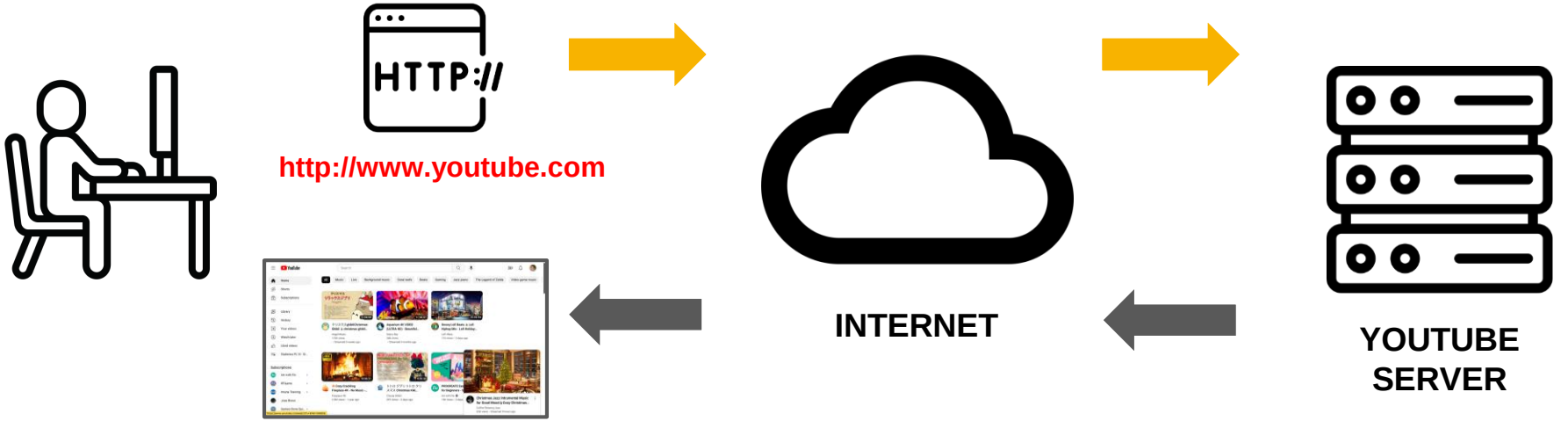
How Does Zscaler Work?

HTTP Overview

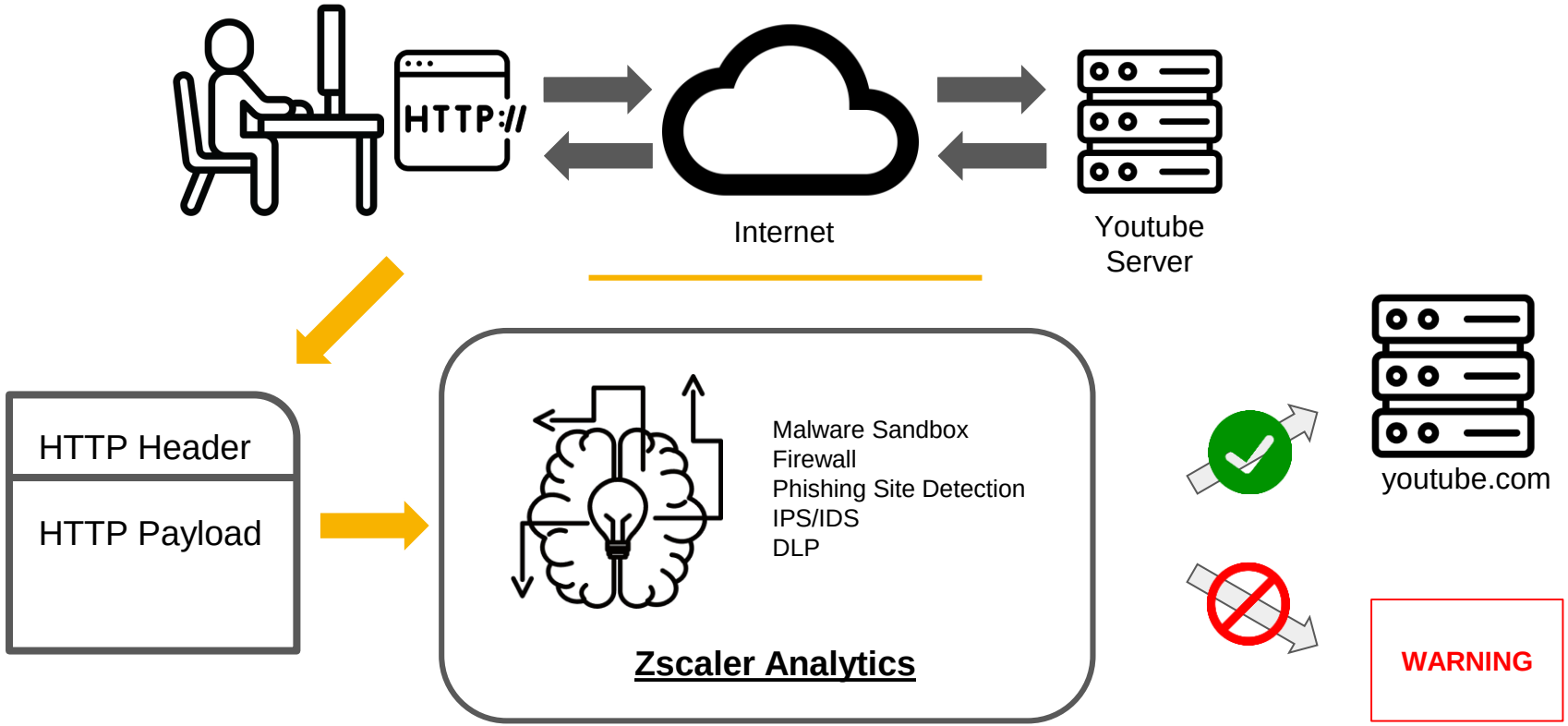


HTTP (Hyper-Text Transfer Protocol)

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



How It Works with Zscaler

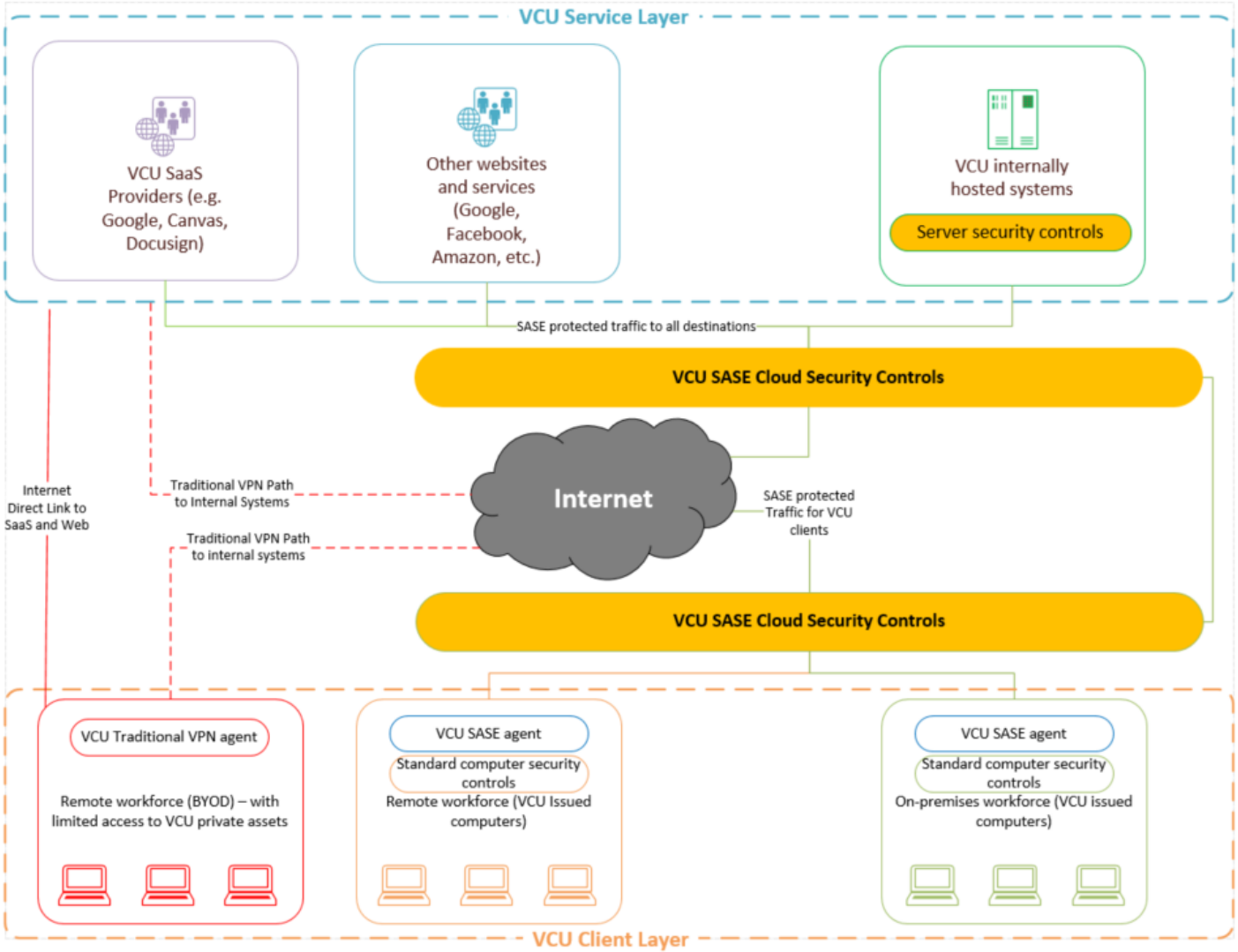


Comparison

	zscaler	
Access VCU Applications?		
Continual Access?		
Detect Malware/Phishing?		
Protect from Harmful Traffic?		

Accomplishes

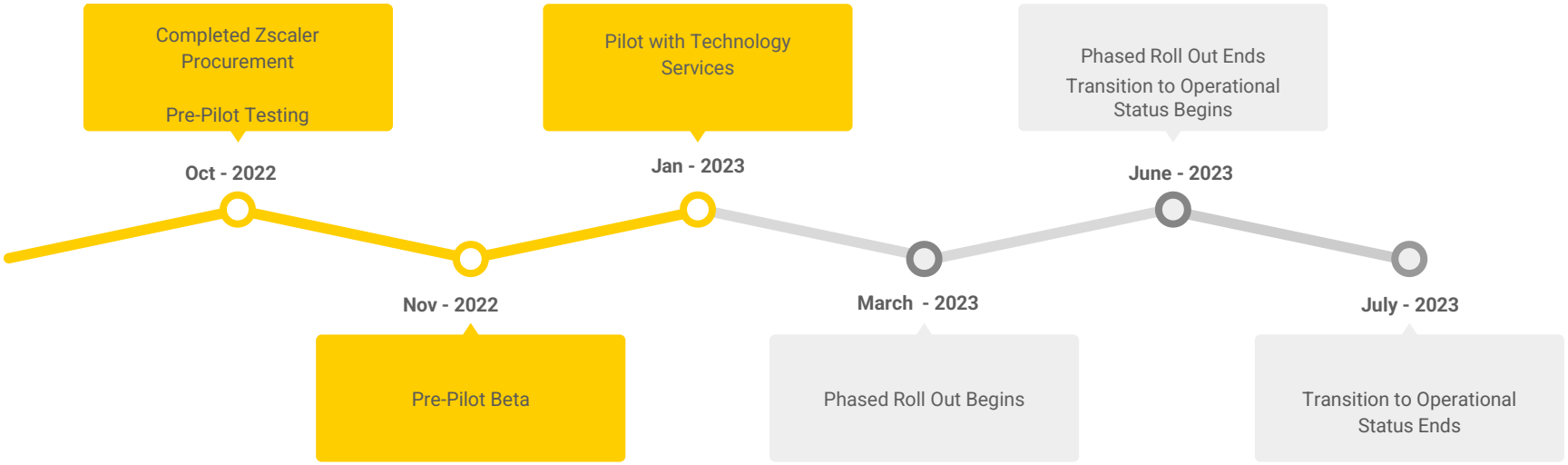
Future VCU Security Model



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