



Cybersecurity Practices in Transportation & Logistics

Michael Ehrich

SVP of Global IT & Security

About Me

Michael Ehrich

SVP, Global IT & Security

project44

Chicago, IL



About project44

The world's leading Advanced Visibility Platform™ for shippers and logistics service providers, project44 (p44) handles the data and analytics of a significant percentage of the global supply chain.

Headquartered in Chicago, IL

860+ Team Members across 25 countries

1,300+
Customers

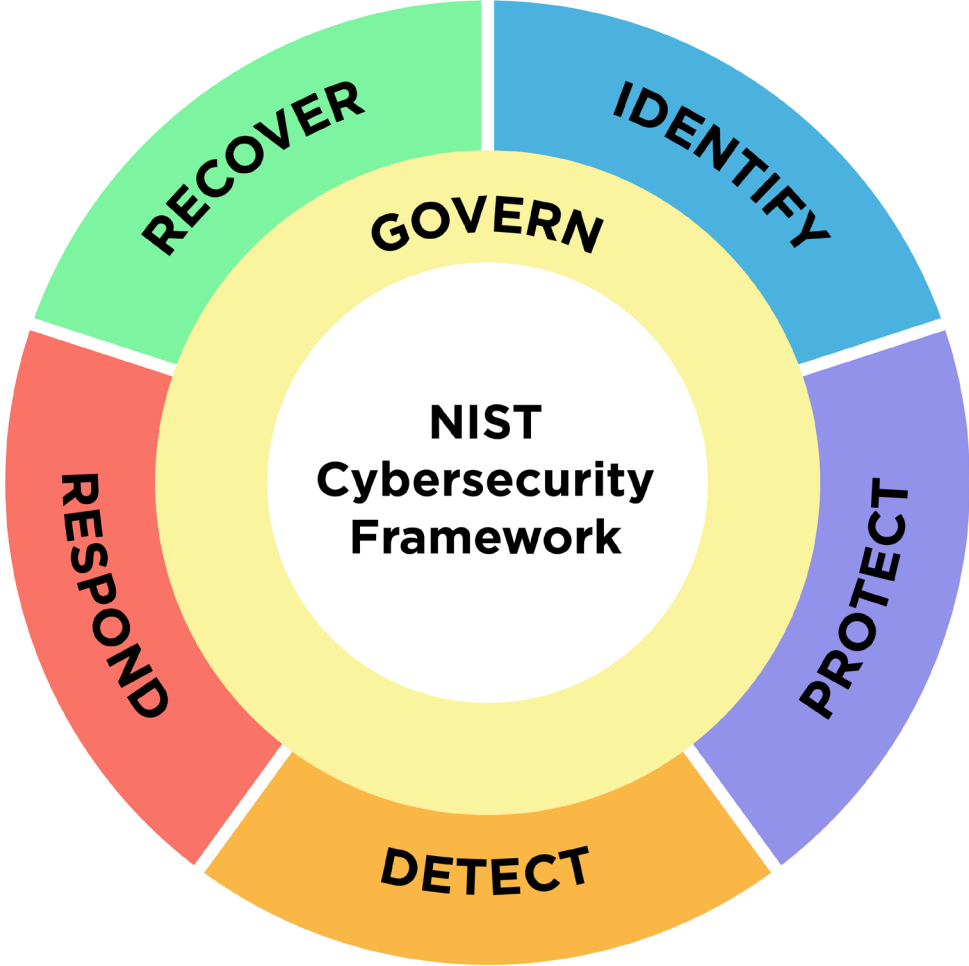
240,000+
Carriers

1B+
Shipments
Tracked
Annually

10B+ Supply
Chain Data
Points per
Month

NIST Cybersecurity Framework 2.0

National Institute of Standards and Technology (NIST)



Customers Trust project44



53 Security Controls



145 Security Controls

What's a Security Control?

- A security control is a process, policy, or standard (safeguards or countermeasures) that mitigate risks and protect assets
- SOC and ISO controls are audited annually by their respective auditors
- project44 also performs an internal audit every six months on these controls



Types of Controls

- Process Controls (non-technical)
- Technical Controls

Examples of Process Controls

1. Penetration Testing DETECT

Examples of Process Controls

1. Penetration Testing 
2. Security Awareness Training 

Examples of Process Controls

1. Penetration Testing DETECT
2. Security Awareness Training PROTECT
3. 3rd Party / Vendor Risk Management IDENTIFY

Product Security

Technical Controls



Examples of Technical Controls – Product Side

1. Encryption in Transit **PROTECT**

2. Encryption at Rest **PROTECT**

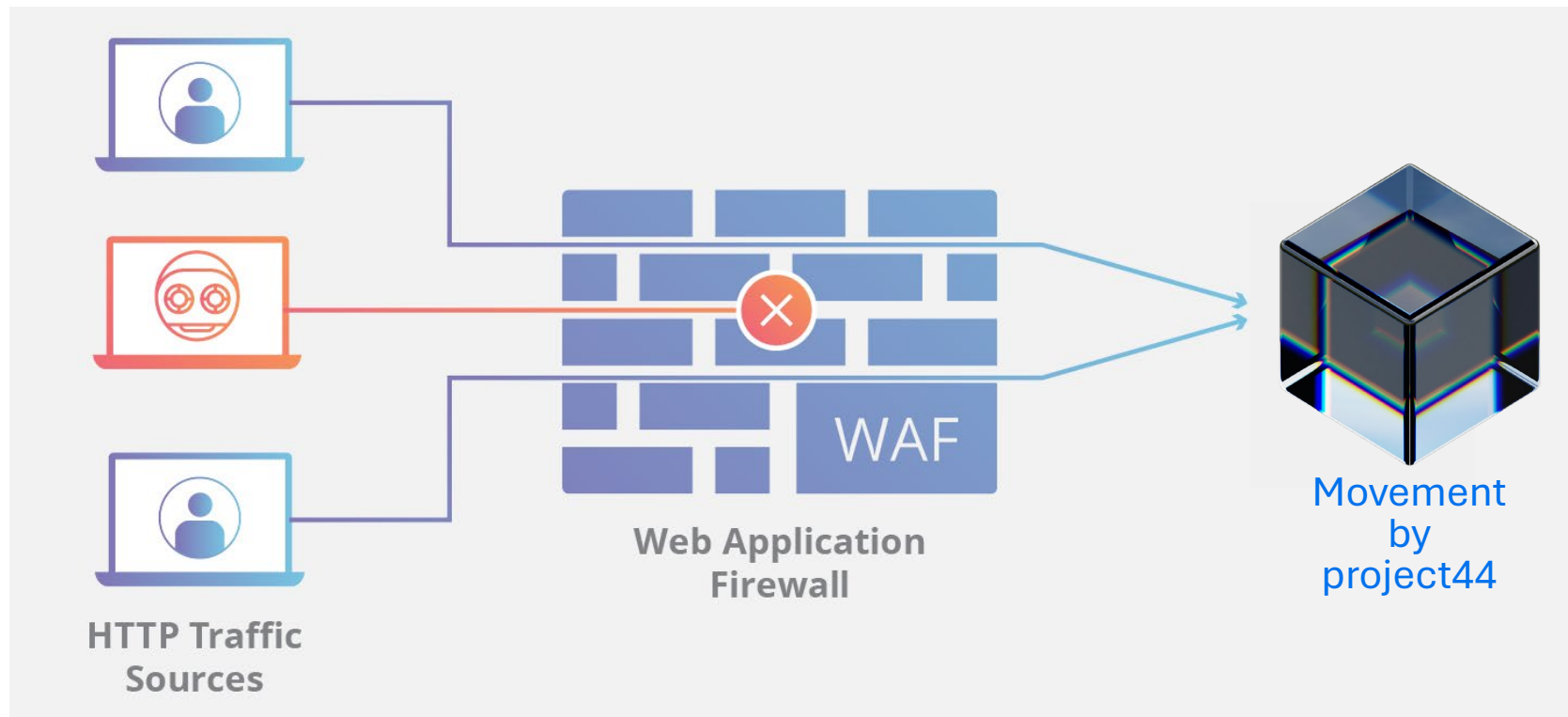
Examples of Technical Controls – Product Side

1. Encryption in Transit PROTECT
2. Encryption at Rest PROTECT
3. Multi-Tenancy Access Control PROTECT

Examples of Technical Controls – Product Side

1. Encryption in Transit **PROTECT**
2. Encryption at Rest **PROTECT**
3. Multi-Tenancy Access Control **PROTECT**
4. Web Application Firewall (WAF) **PROTECT**

Web Application Firewall (WAF)



Examples of Technical Controls – Product Side

1. Encryption in Transit **PROTECT**
2. Encryption at Rest **PROTECT**
3. Multi-Tenancy Access Control **PROTECT**
4. Web Application Firewall (WAF) **PROTECT**
5. Multi-Region Replication **RECOVER**

Examples of Technical Controls – Product Side

1. Encryption in Transit **PROTECT**
2. Encryption at Rest **PROTECT**
3. Multi-Tenancy Access Control **PROTECT**
4. Web Application Firewall (WAF) **PROTECT**
5. Multi-Region Replication **RECOVER**
6. Backups & DR **RECOVER**

Examples of Technical Controls – Product Side

1. Encryption in Transit **PROTECT**
2. Encryption at Rest **PROTECT**
3. Multi-Tenancy Access Control **PROTECT**
4. Web Application Firewall (WAF) **PROTECT**
5. Multi-Region Replication **RECOVER**
6. Backups & DR **RECOVER**
7. System Patching **RESPOND**

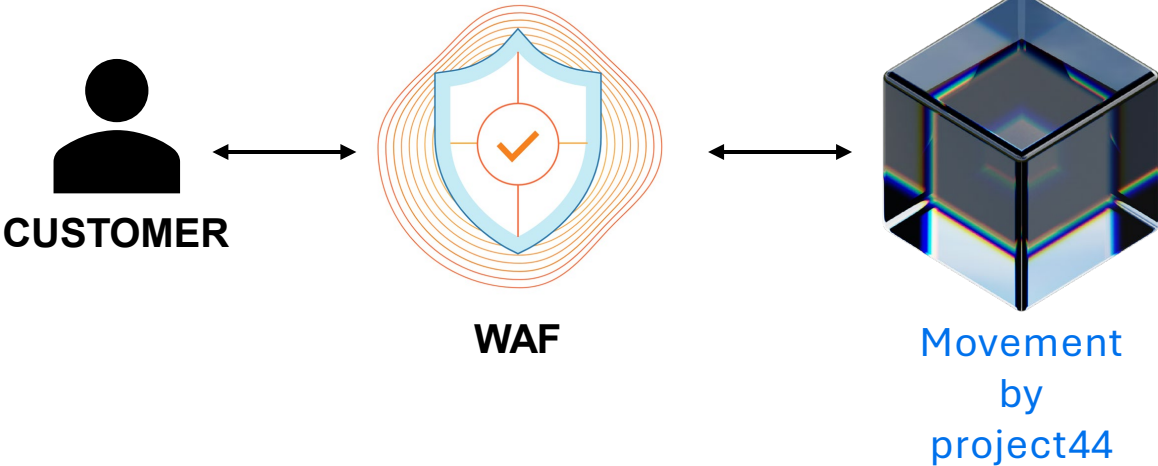
Internal Security

Technical Controls

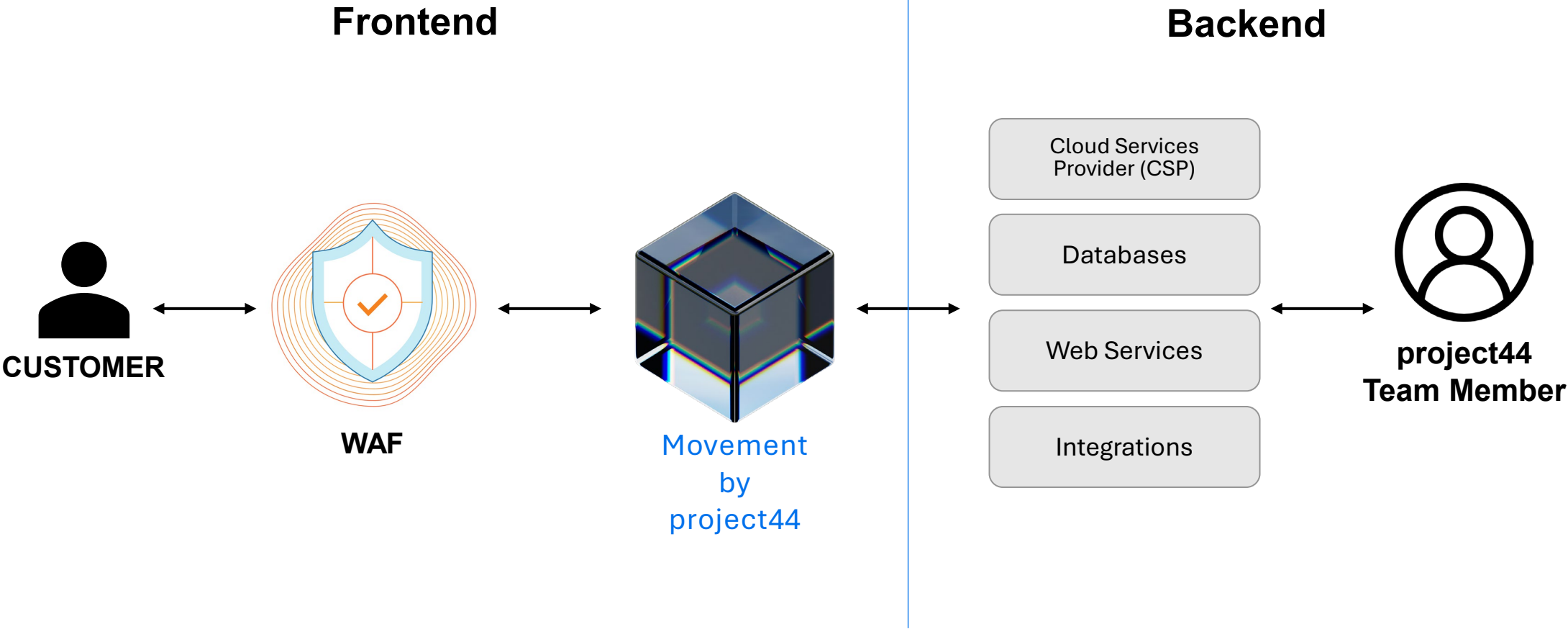


SaaS Design

Frontend



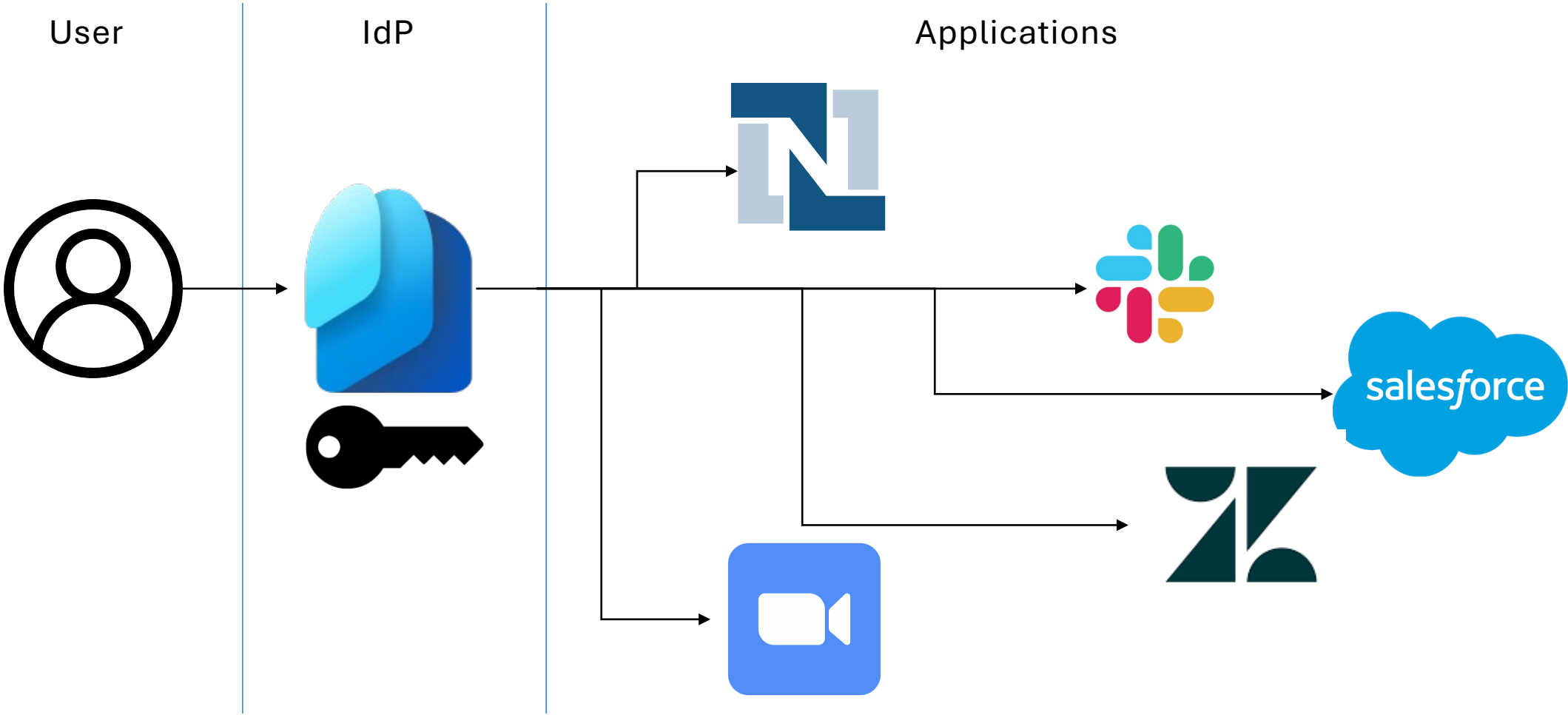
SaaS Design



Examples of Technical Controls - Internal

1. Unified Login (SSO) PROTECT

With SSO



Without SSO



Examples of Technical Controls - Internal

1. Unified Login (SSO) **PROTECT**

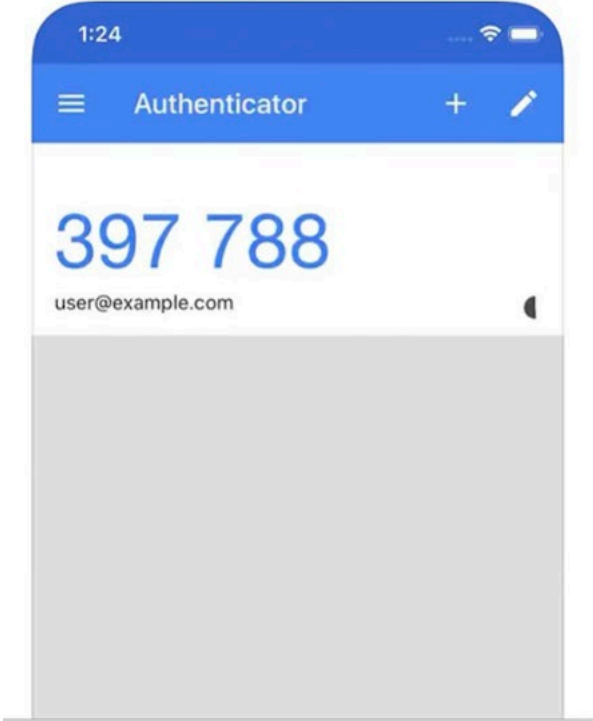
2. Multifactor Authentication (MFA) **PROTECT**

MFA SMS (Text)

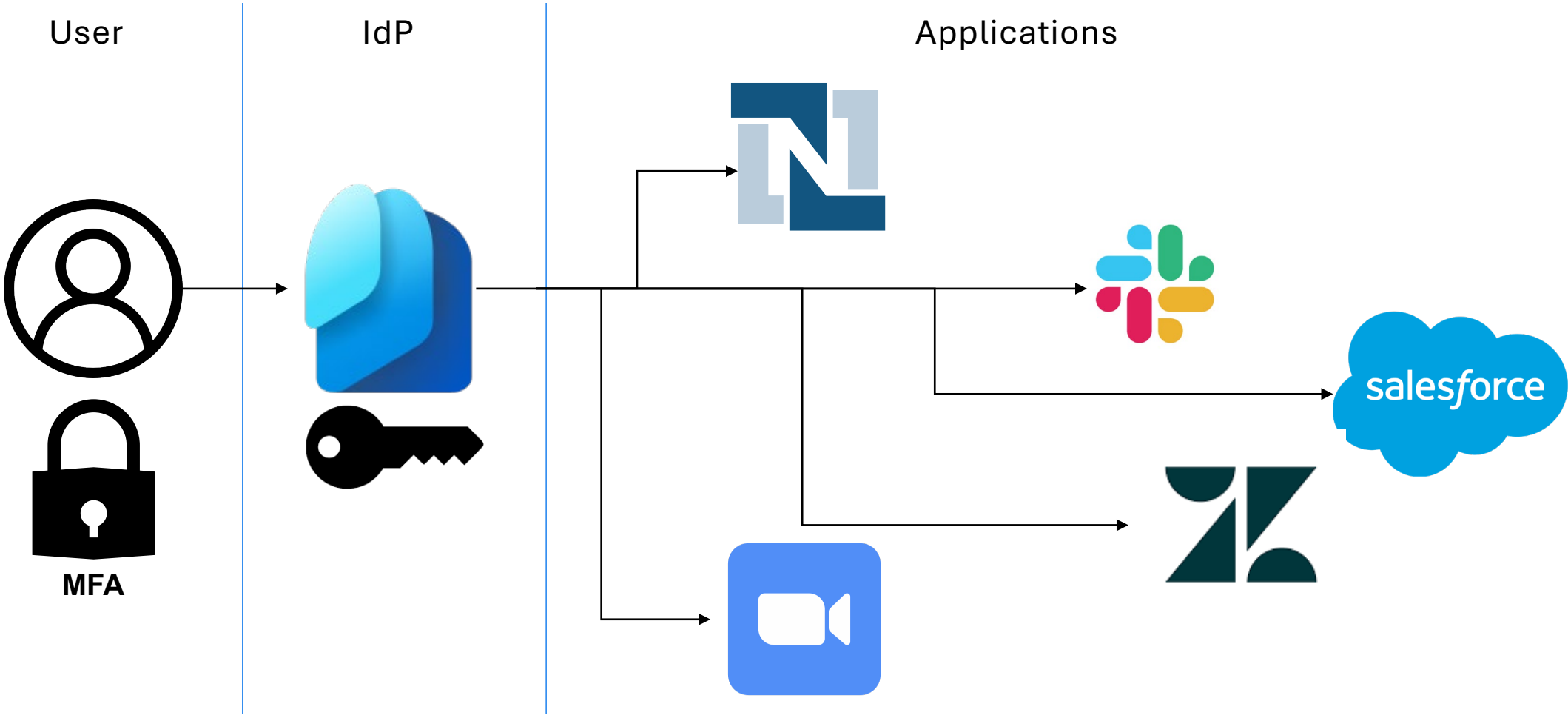
Wells Fargo will NEVER call or text you for this code. DON'T share it. Enter Advanced Access code 365600 online to verify your identity.

Your E*TRADE verification code is 469269. No one from E*TRADE will contact you for this code unless initiated by you. Didn't request a code? Call [1-800-387-2331](tel:1-800-387-2331)

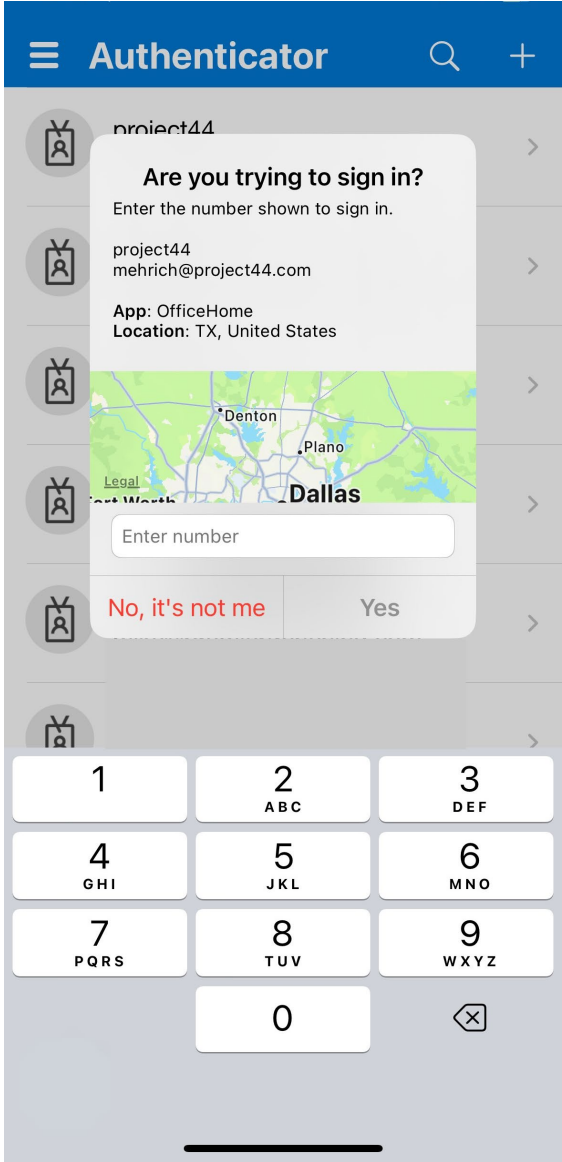
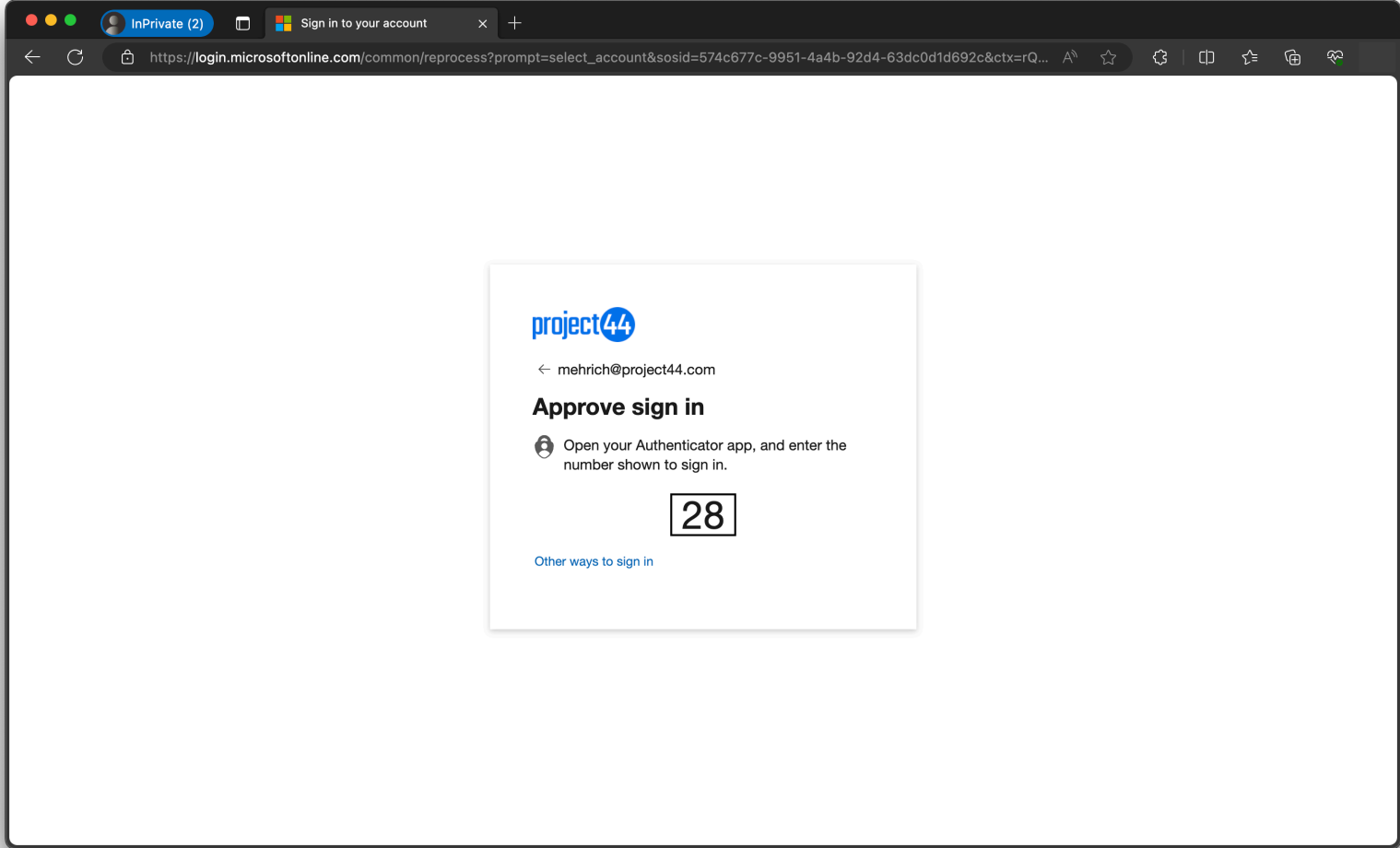
MFA Rolling Codes



SSO with MFA



Passwordless Sign-in



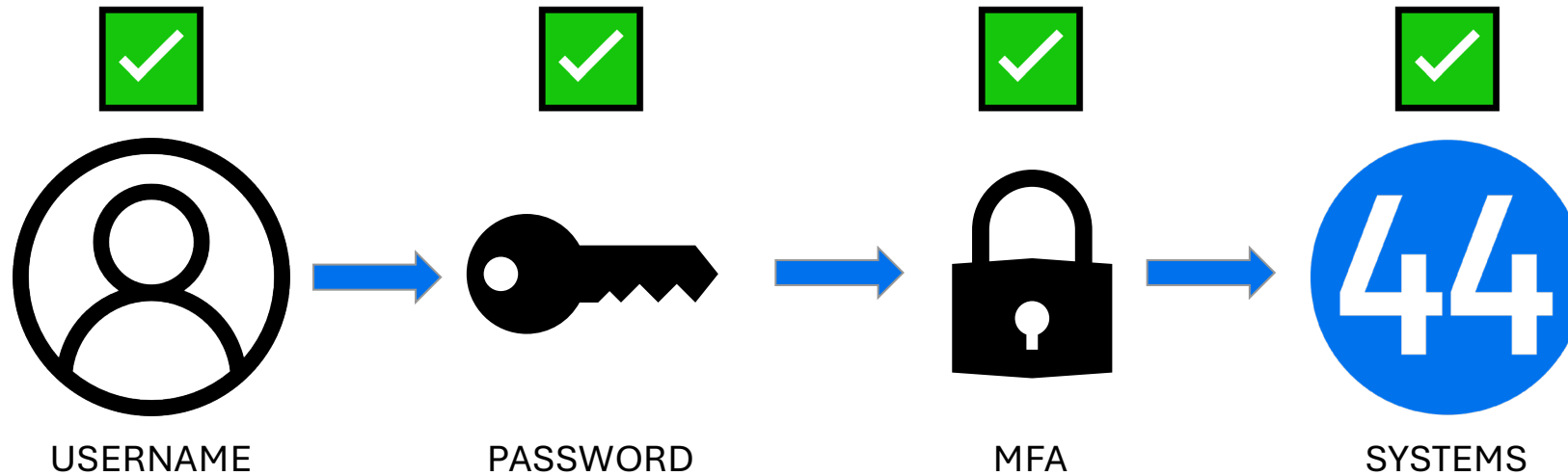
FIDO2 Keys



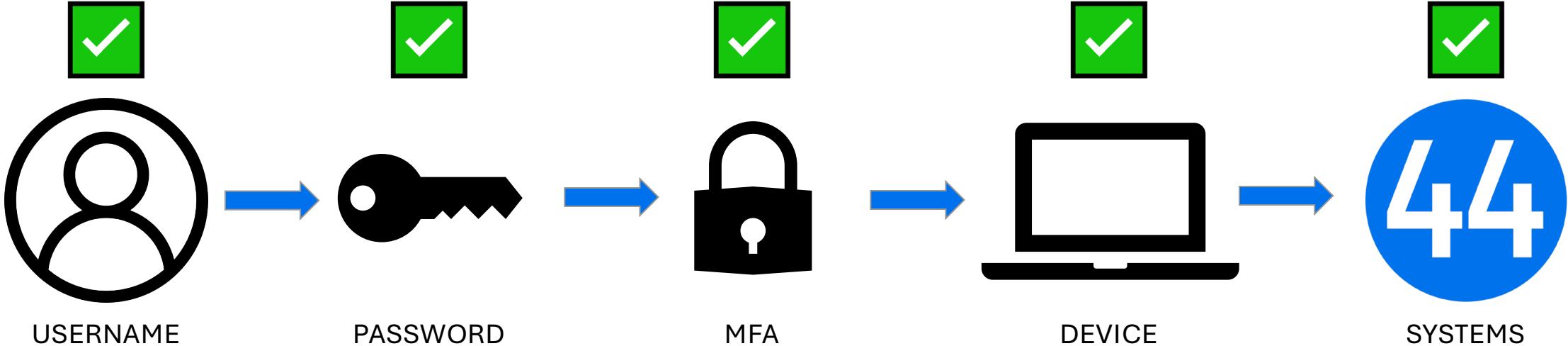
Examples of Technical Controls - Internal

1. Unified Login (SSO) PROTECT
2. Multifactor Authentication (MFA) PROTECT
3. Trusted Devices PROTECT IDENTIFY
 - a. Serial number match via Autopilot / ABM
 - b. Enrolled and managed by project44 EDM (Endpoint Device Management)
 - c. Full Disk Encryption
 - d. Antivirus/Anti-Malware installed and updated
 - e. Automated patching
 - f. Other project44-specific policies / restrictions

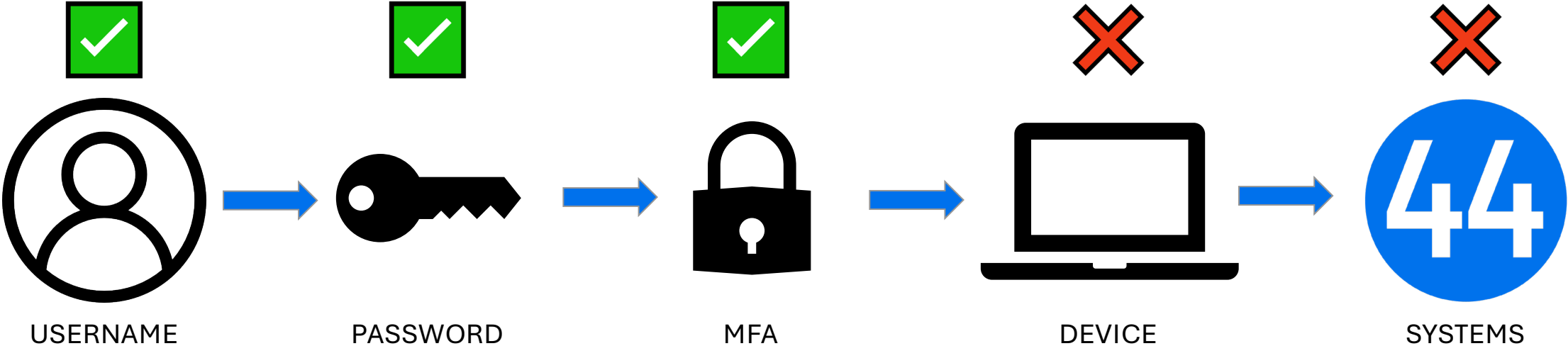
Without Device Compliance



With Device Compliance



No Compliant Device?



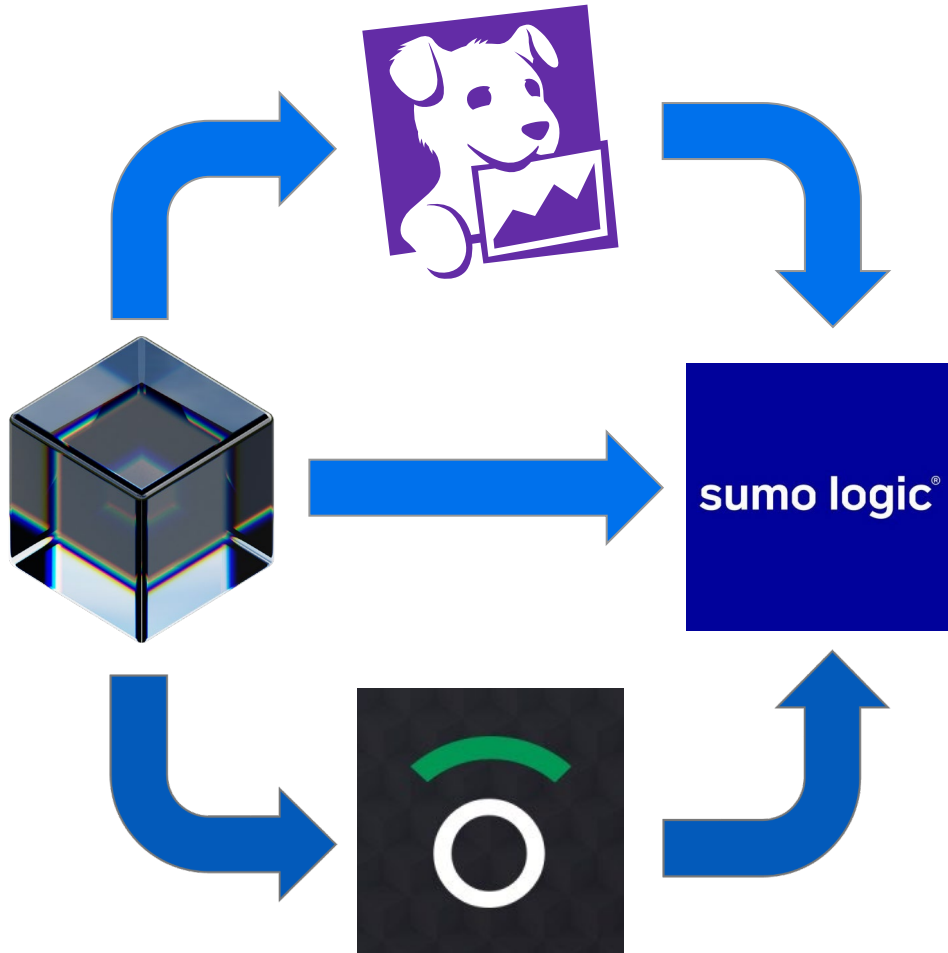
Detect & Respond

DETECT

RESPOND



Monitoring DETECT



24x7 Incident Response RESPOND

- Suspicious / unauthorized login attempts
 - Platform & Internal Systems
- Logins from suspicious IPs or locations
- Landspeed (impossible travel) violations
- Malicious URLs in emails
- Carrier outages

Threat intelligence from sources such as:

- Microsoft, Crowdstrike, Cloudflare, and VirusTotal

Summary





NIST Cybersecurity Best Practices

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
<ul style="list-style-type: none"> Asset Management Vendor Risk Management 	<ul style="list-style-type: none"> Security Awareness Training Encryption in Transit Encryption at Rest Multi-Tenancy Access WAF Unified Login (SSO) MFA Trusted Devices 	<ul style="list-style-type: none"> Penetration Testing SIEM Monitoring 	<ul style="list-style-type: none"> System Patching 24x7 Incident Response 	<ul style="list-style-type: none"> Multi-Region Replication Backups Disaster Recovery
<p style="text-align: center;">GOVERN Policies, Processes, Procedures, Compliance (SOC 2 Type 2, ISO 27001)</p>				

An aerial photograph of a winding asphalt road through a dense forest. The trees are in various shades of green and yellow, suggesting an autumn setting. A white dashed line runs along the edge of the road. A small blue car is visible on the road, navigating a curve. The text 'project 44' is overlaid in the center of the image. 'project' is in a white, lowercase, sans-serif font, and '44' is in a bold, black, sans-serif font inside a white circle.

project 44