okta

Zero Trust Town

Age
5-99 yrs

179
Pieces

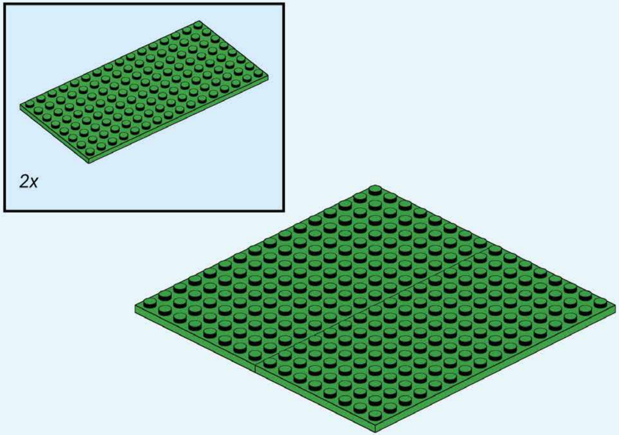
Make identity the foundation for your Zero Trust strategy

Identity is the core of a Zero Trust strategy. In recent years, we've seen the perimeter moving to the identity layer and a rise in identity-based cyber attacks. As a result, people are now the most critical component.

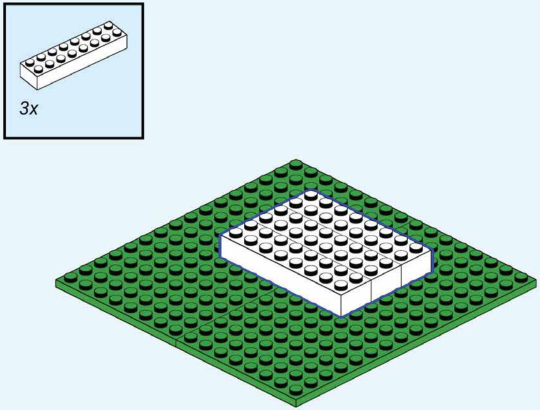
Most organisations progress through several stages of maturity in order to advance their Zero Trust security strategy. Take an abbreviated journey with us as you implement a Zero Trust security approach in Zero Trust Town.

Let’s see how an identity-first approach protects Zero Trust Town.

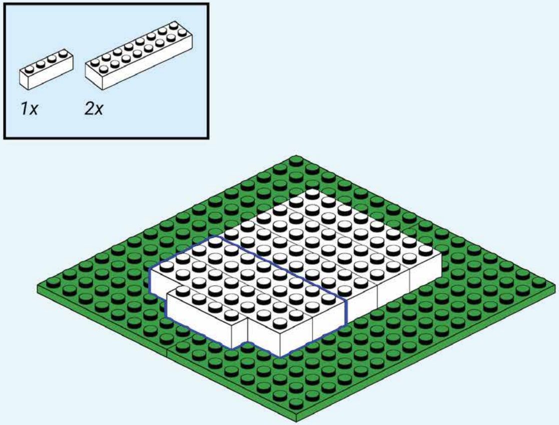
1



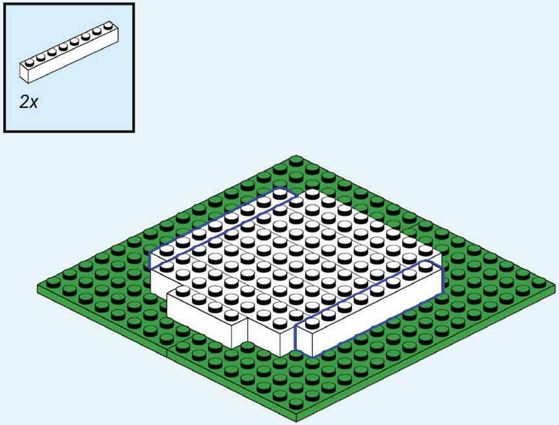
2



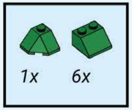
3

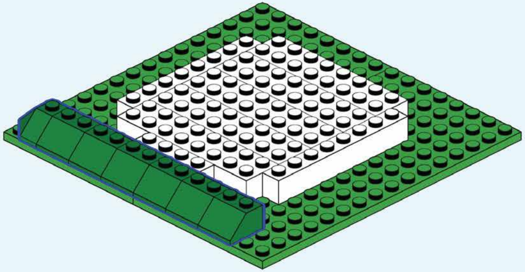


4

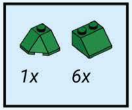


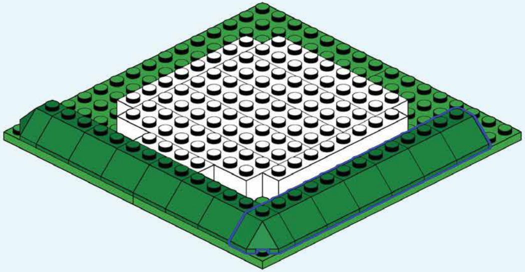
5



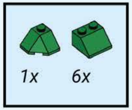


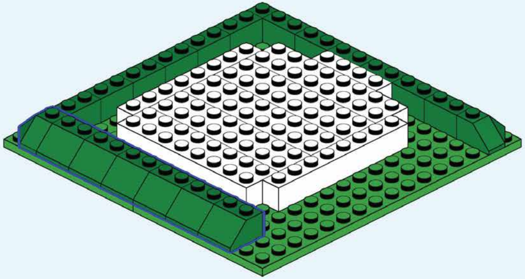
6



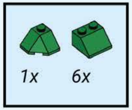


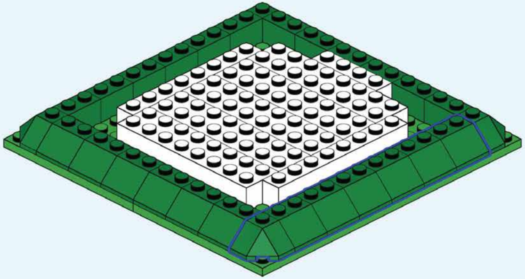
7



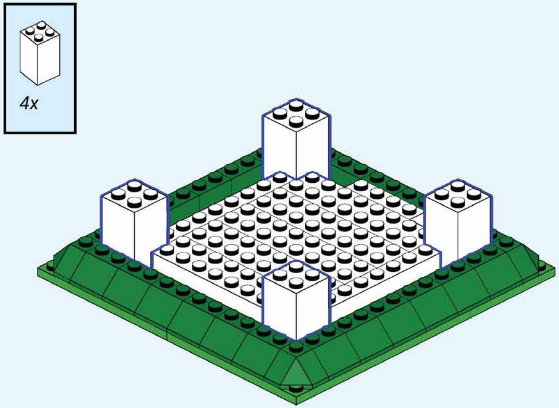


8

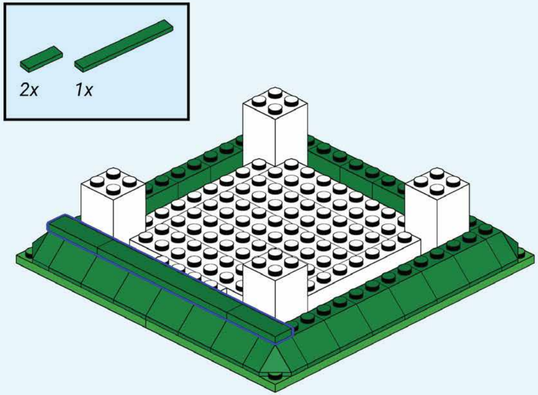




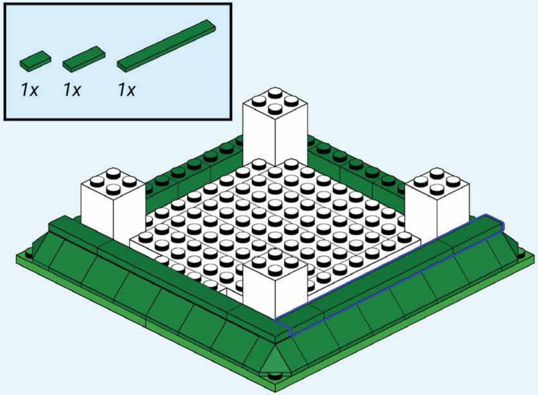
9



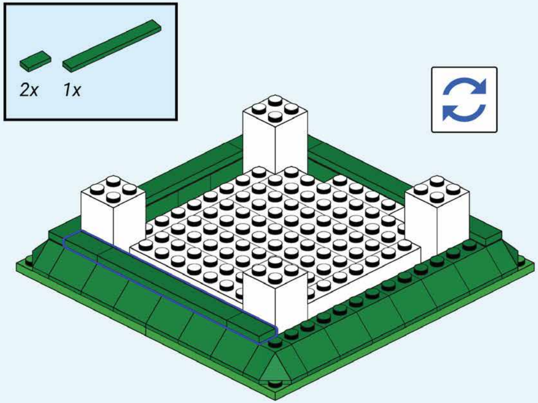
10



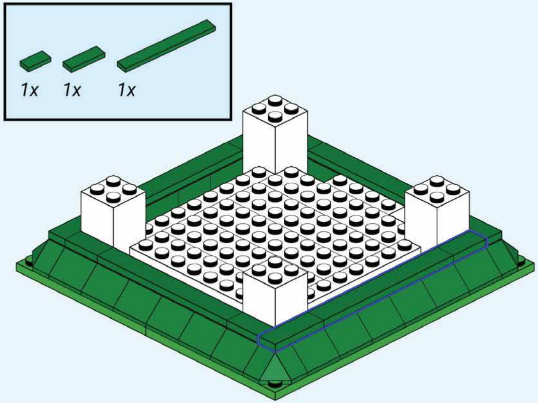
11



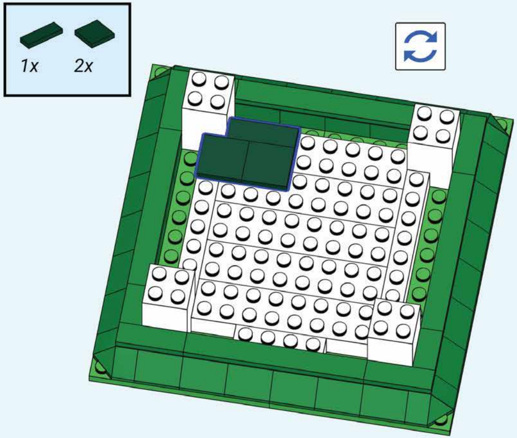
12



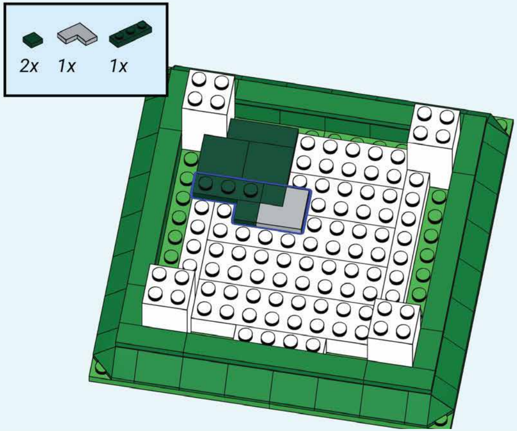
13



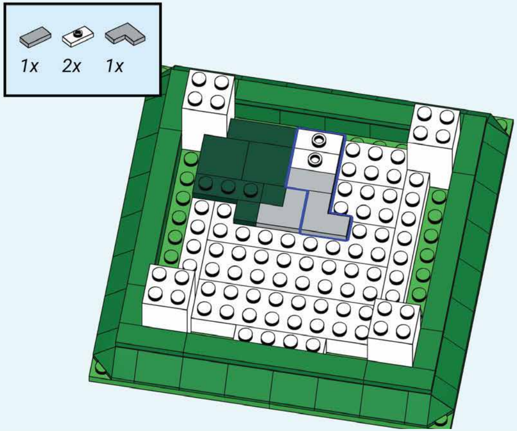
14



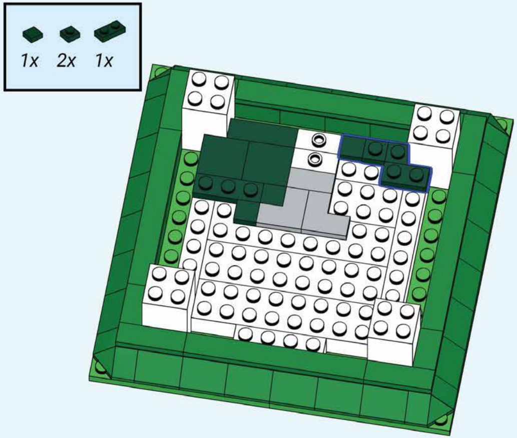
15



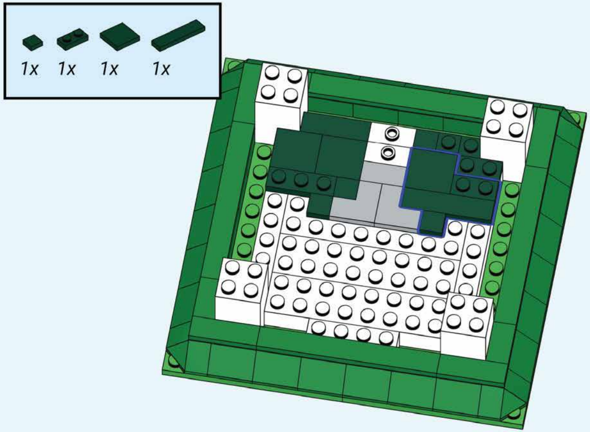
16



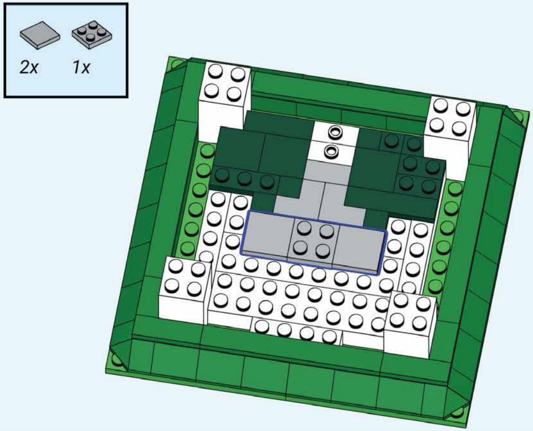
17



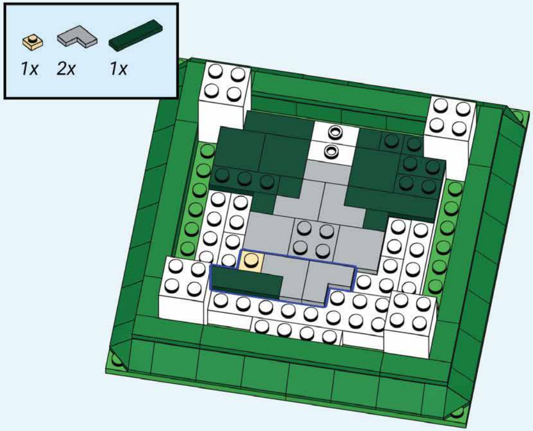
18



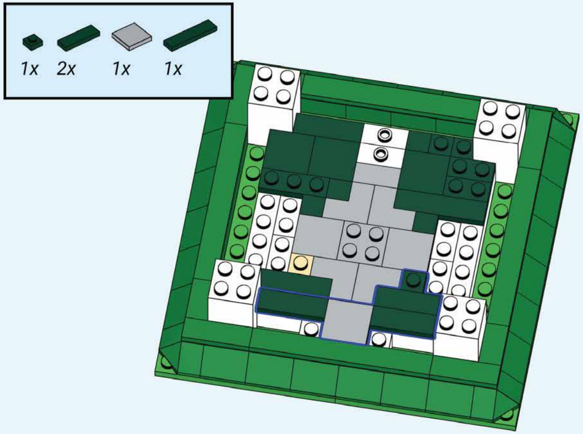
19



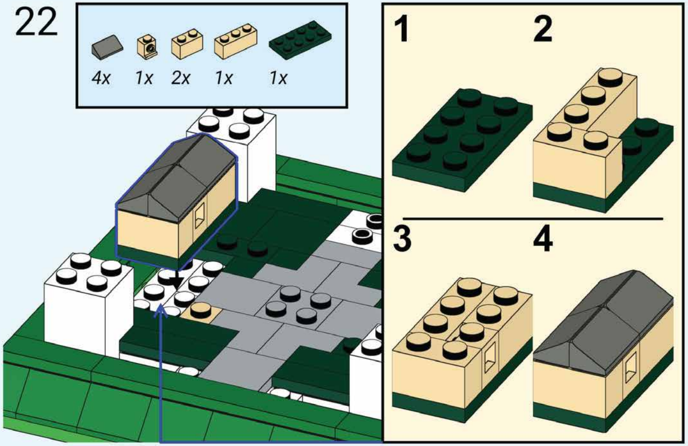
20



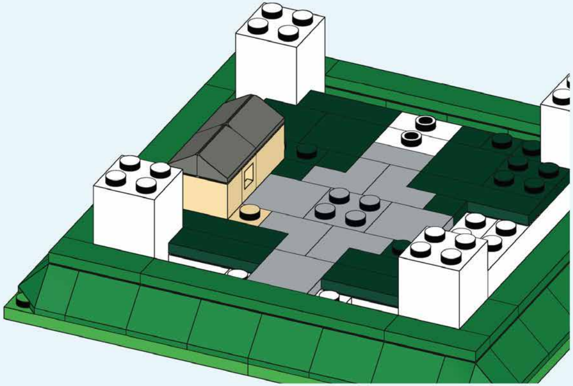
21



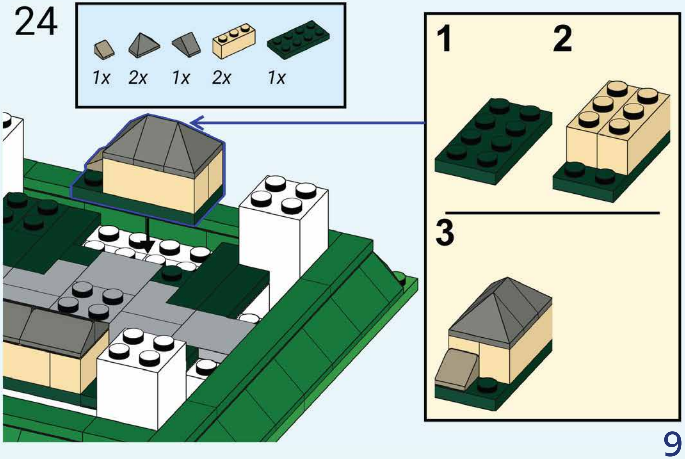
22



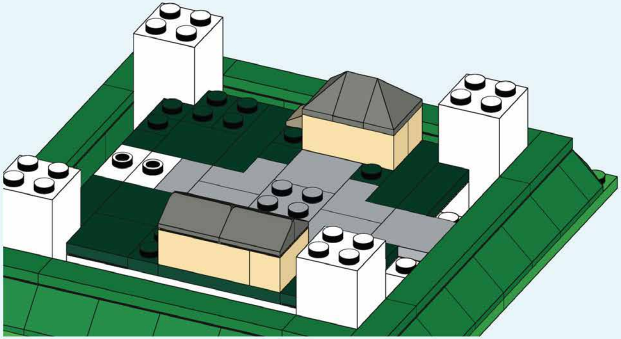
23



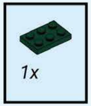
24

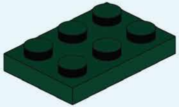


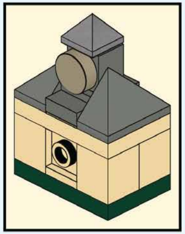
25



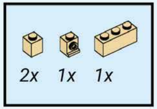
26

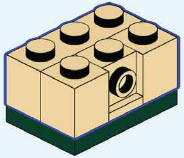




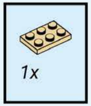


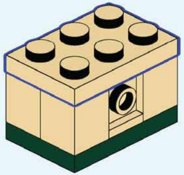
27



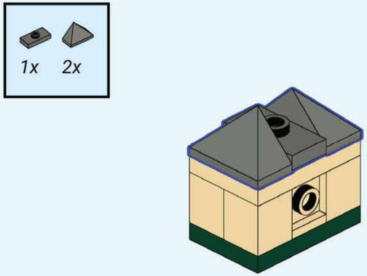


28

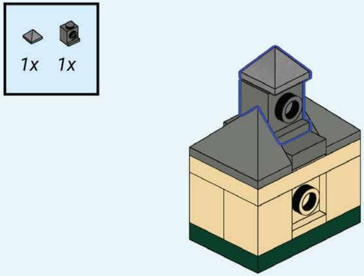




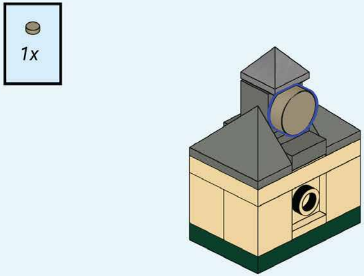
29



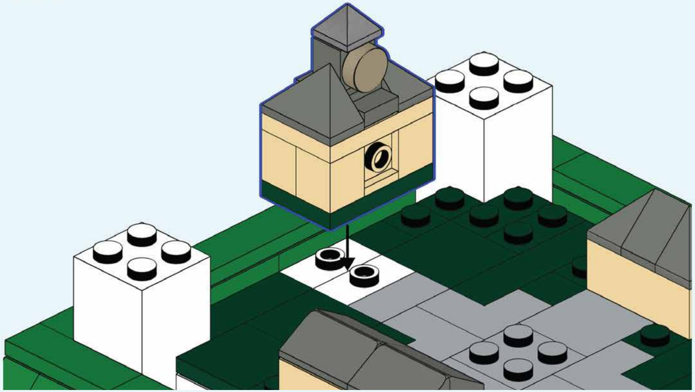
30



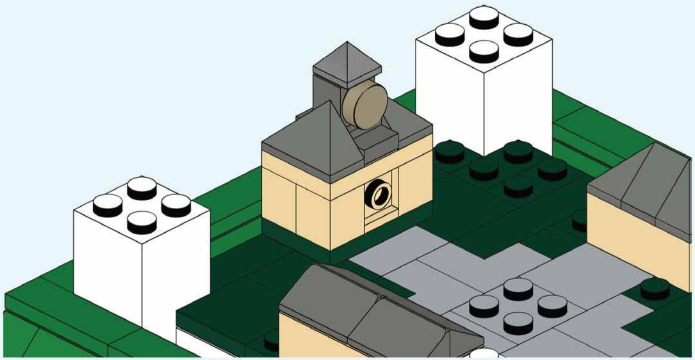
31



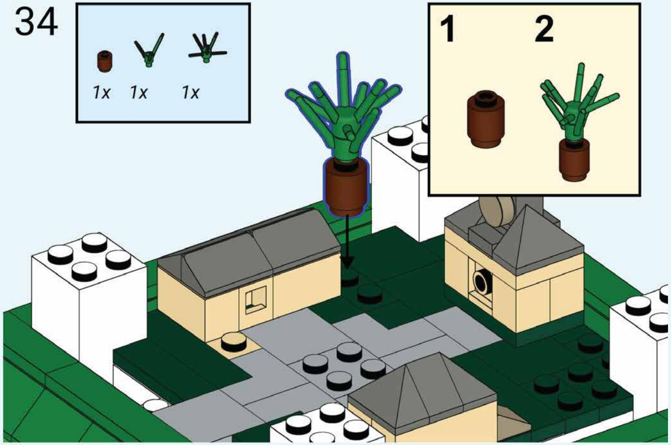
32



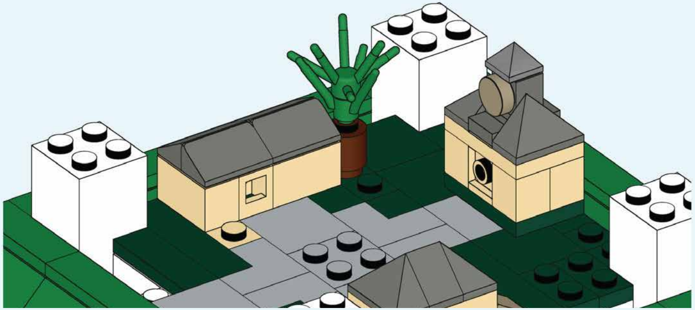
33



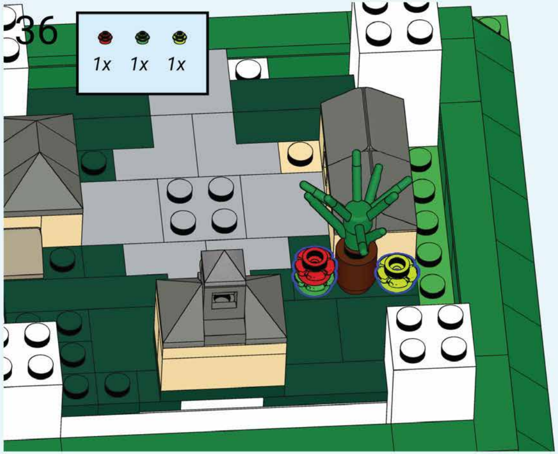
34



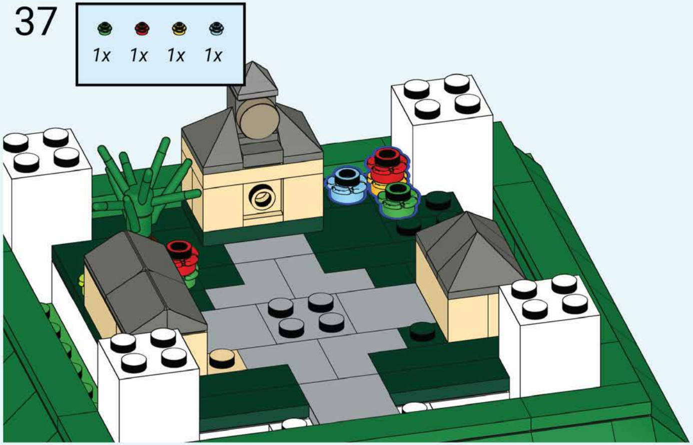
35



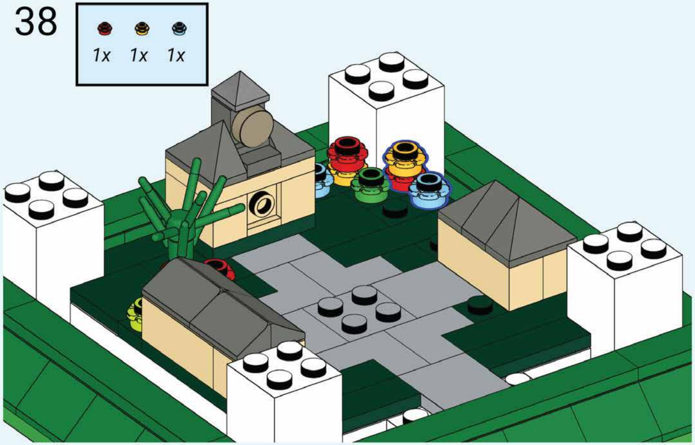
36



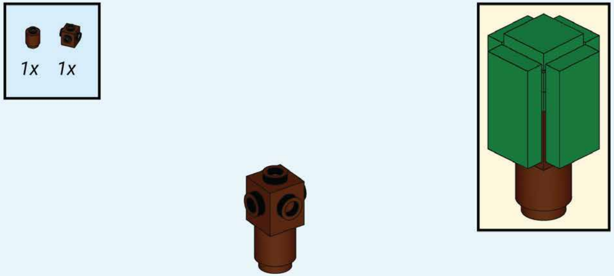
37



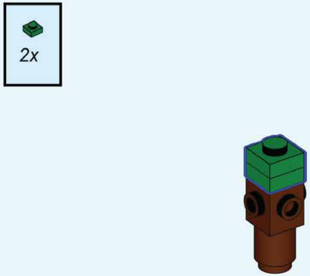
38



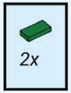
39

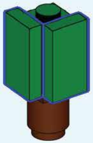


40

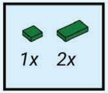


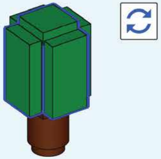
41



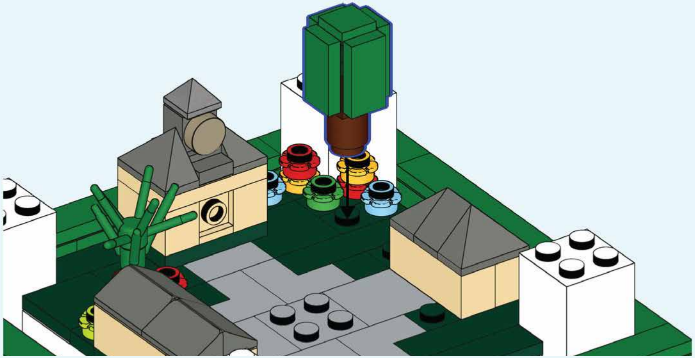


42

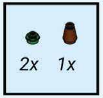


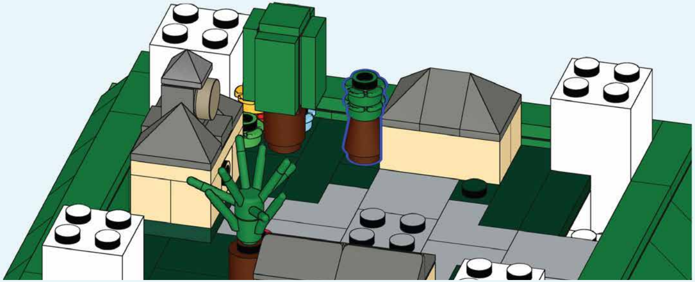


43

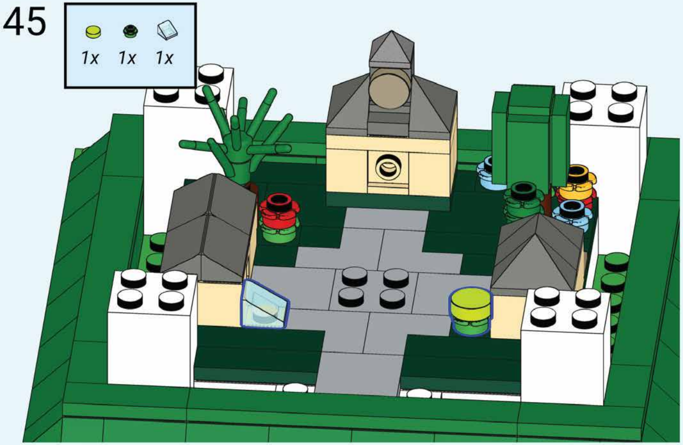


44

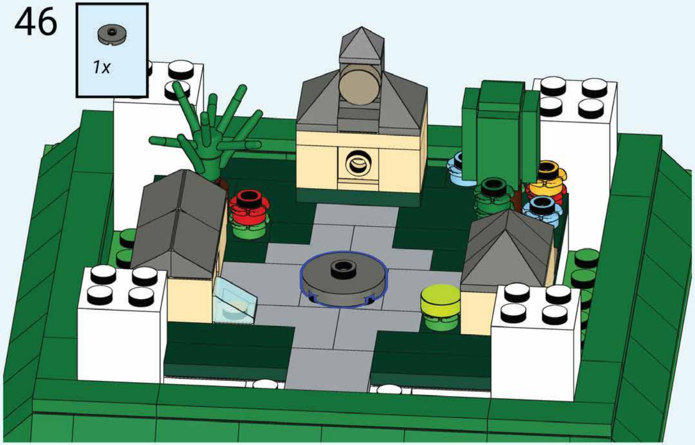




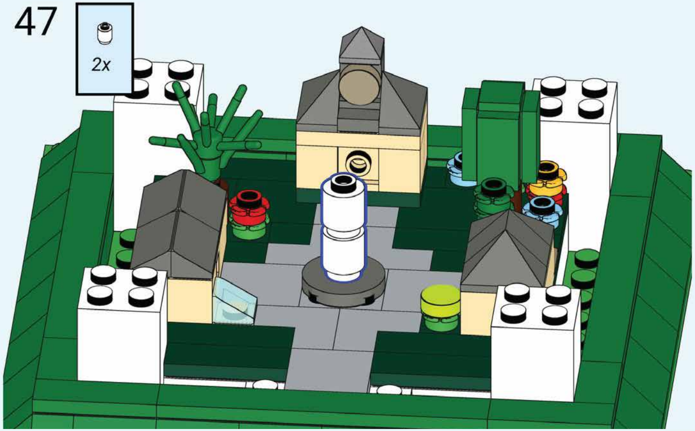
45



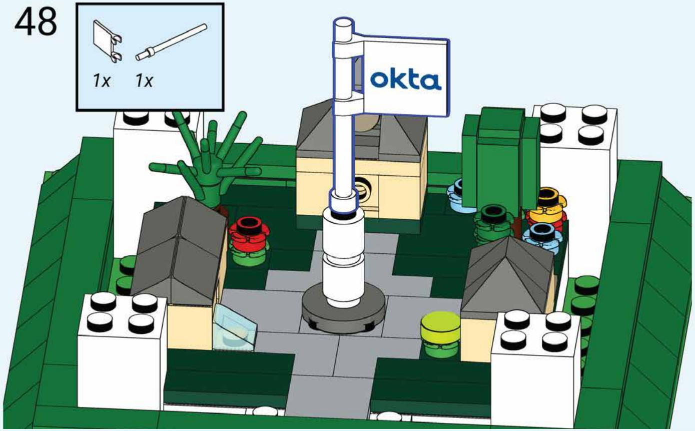
46



47



48

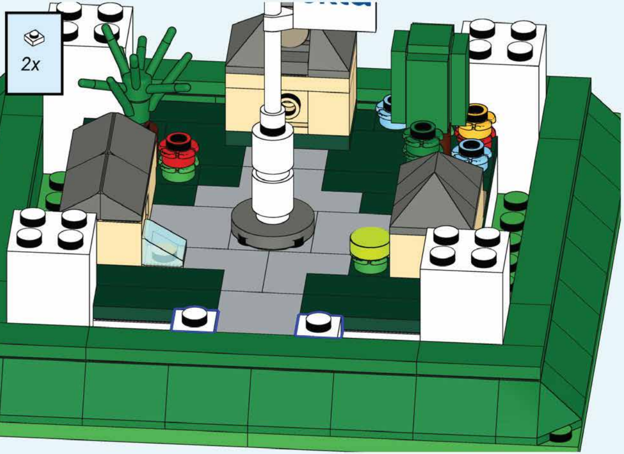


Something to protect

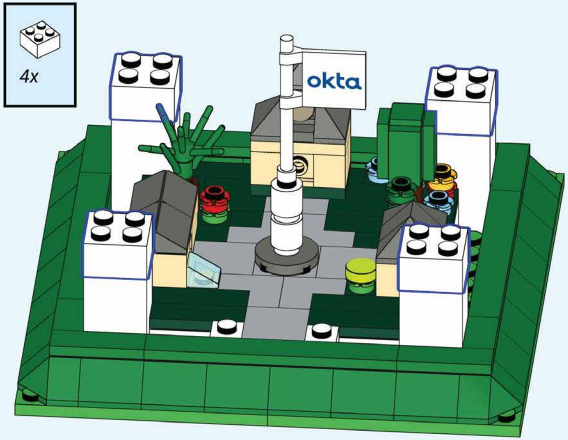
You've put blood sweat and tears into building your site and town. There's really something to protect here, but over time the town was built using disparate materials – some were found on-premise and some beyond the town walls. It's become difficult to maintain the fragmented pieces and you stand vulnerable to attackers.

Many organisations are built in a similar fashion – as we scale we bring on a variety of on-premise and cloud applications that are not fully integrated. IT is forced to manage disparate identities across a number of systems as well as the many applications and services. Without visibility and ownership over these fragmented identities, IT and security teams are left with potentially large windows for attackers to exploit.

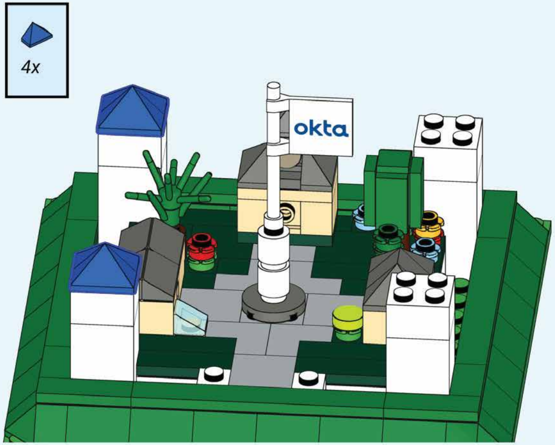
49



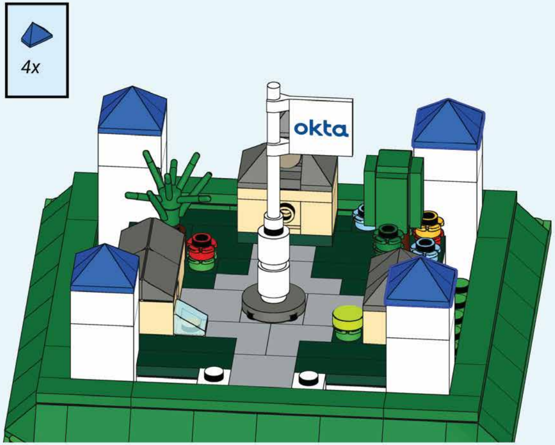
50



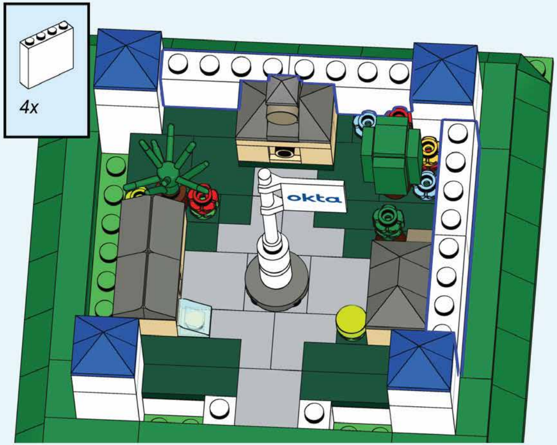
51



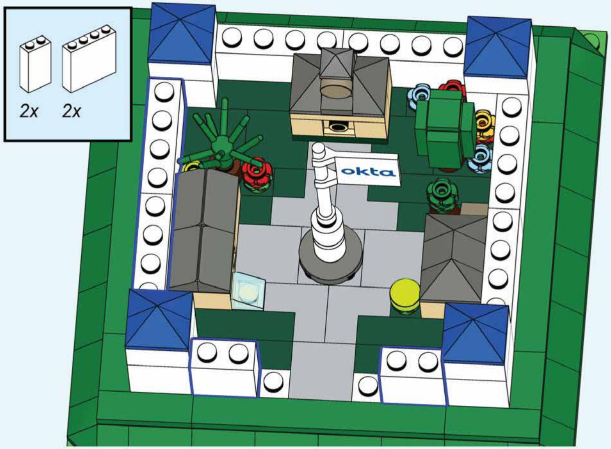
52



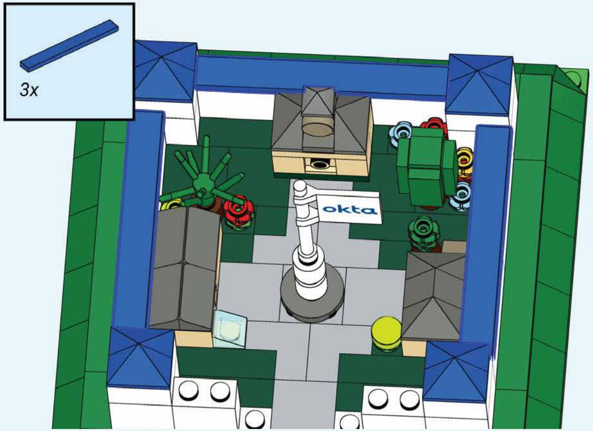
53



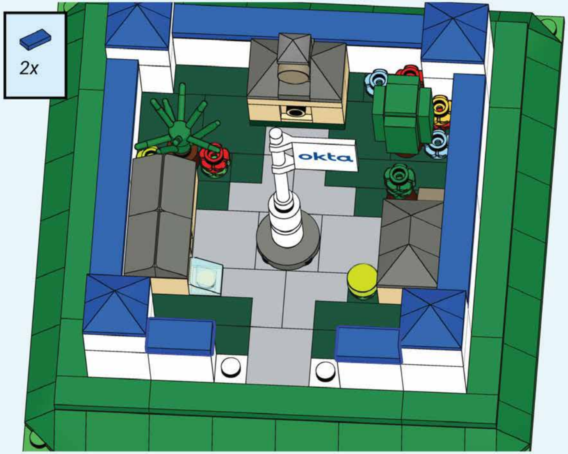
54



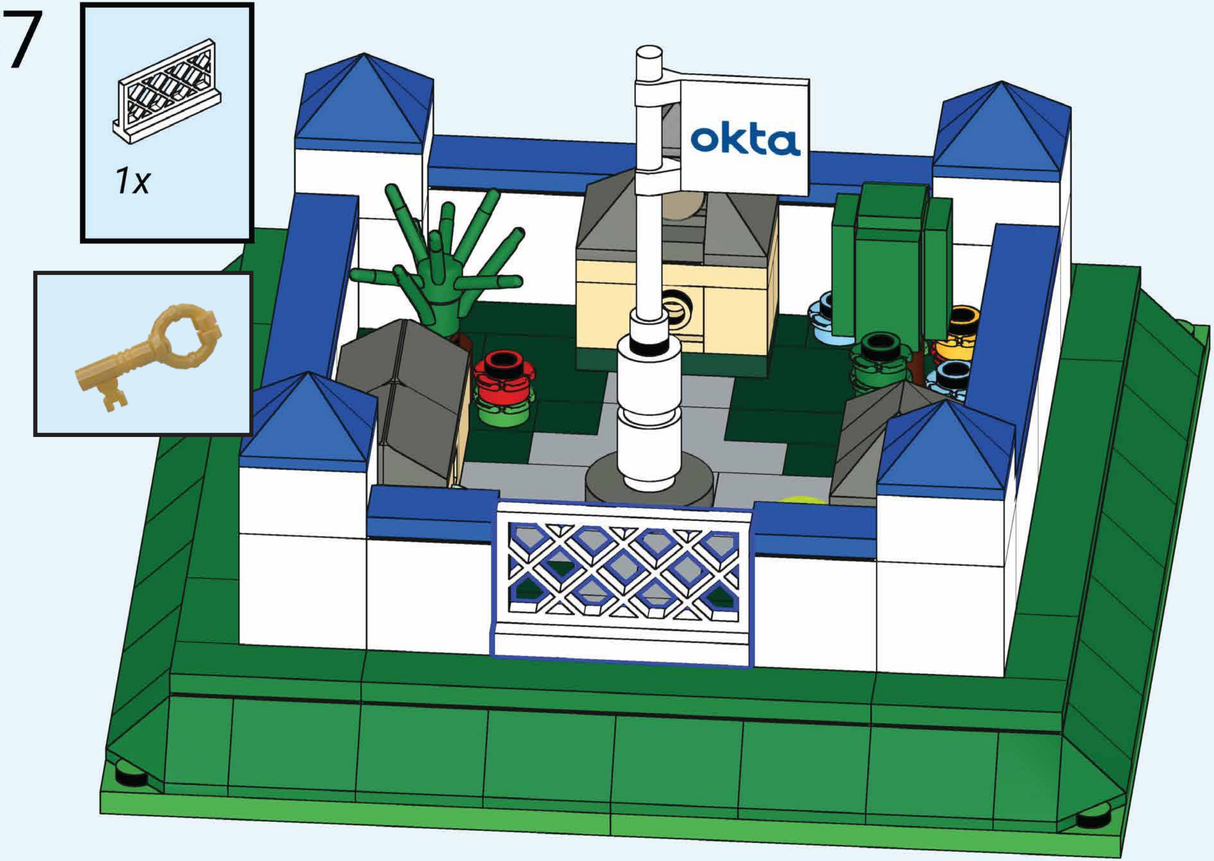
55



56



57



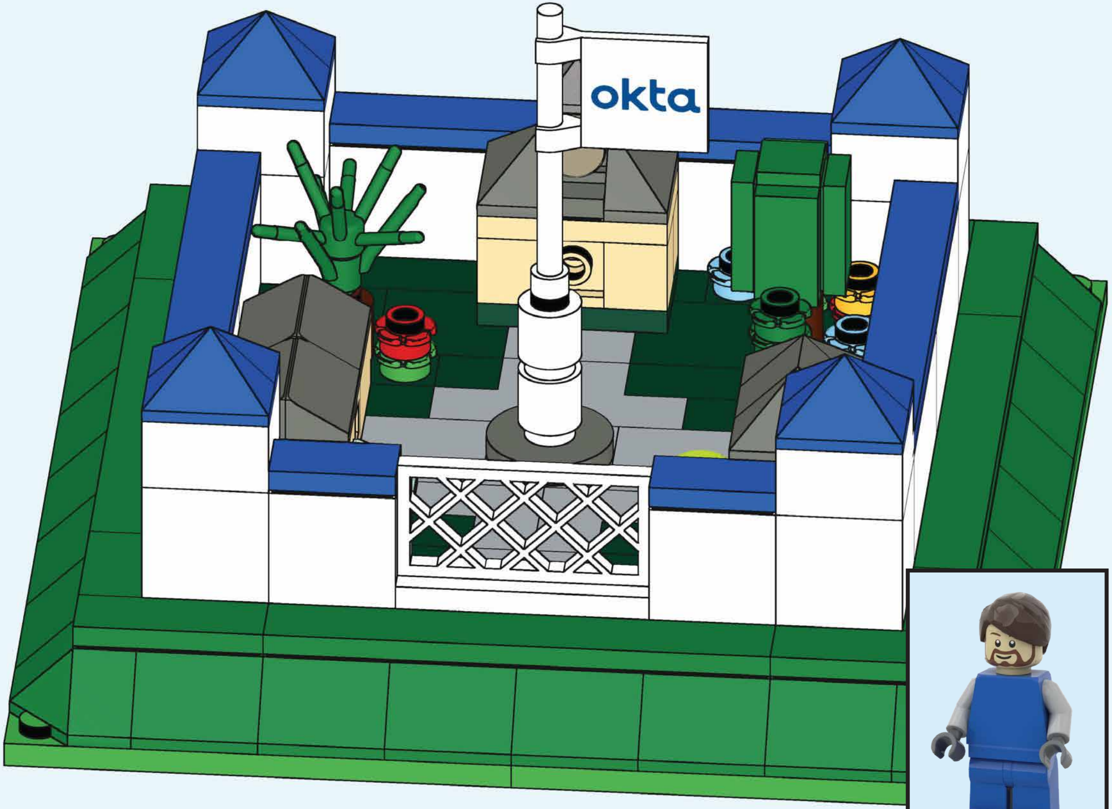
STAGE 1: Unified Identity and Access Management

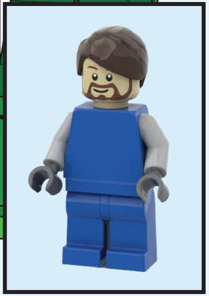
Under lock and key

Congratulations, all your buildings are connected to a solid base and you've built a sturdy wall with a single point of access. It's become a lot easier to manage and protect your town – only people with a key may enter!

You can probably draw the parallel to your security architecture – unifying identity makes it much easier for IT to manage access to the full breadth of on-premise and cloud resources. A centralised identity access point helps to further mitigate attacks targeting credentials.

58





STAGE 2: Contextual Access

Upgrade to Guard Duty

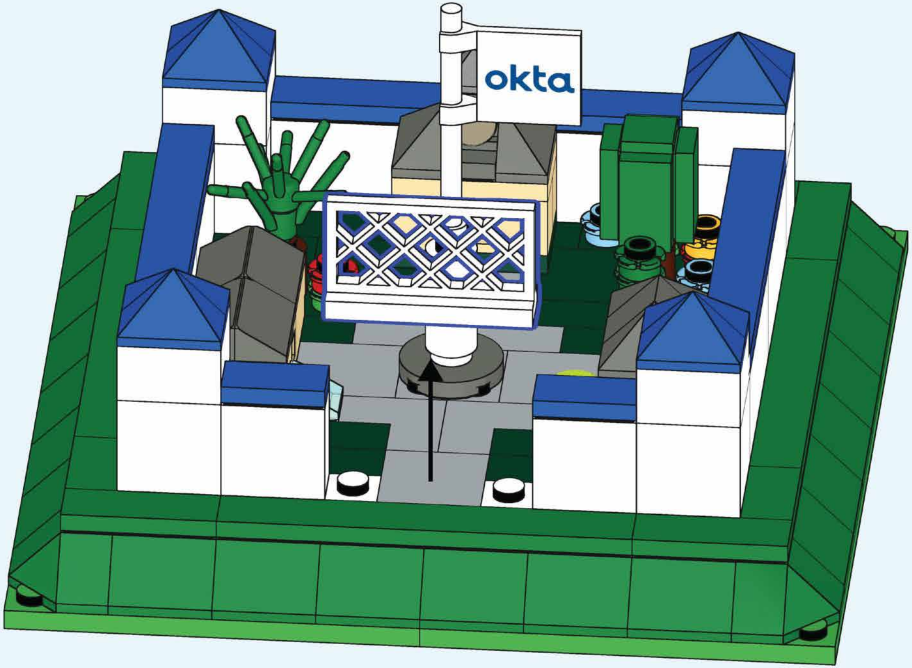
For a while there was peace in the town, it was easy to see who was coming and going and to enter all you needed was a key to the town. Unfortunately, an intruder was able to get through the gate by obtaining a key and resources were stolen!

Taking immediate action, you built a more fortified gate and put a guard on duty. Now, if a person enters the town and triggers a warning, a guard will ask more context-based questions before providing access. The town's motto has become 'trust no one, always verify.'

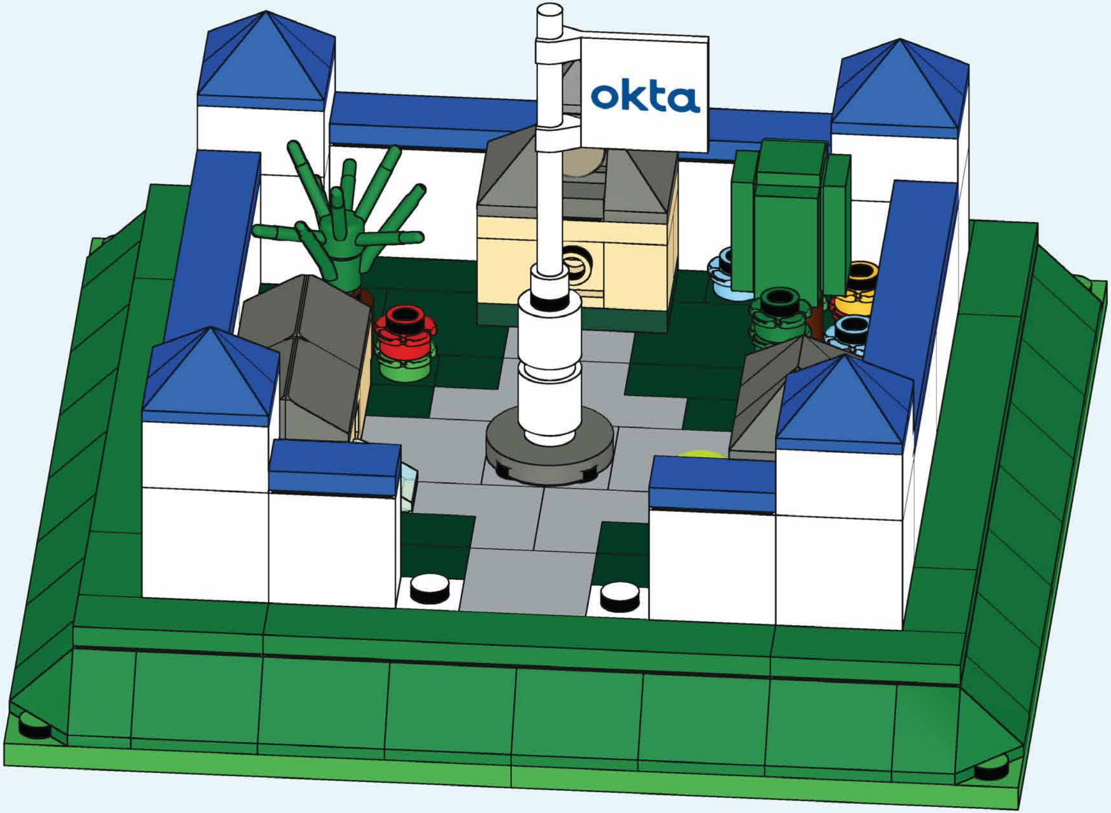
In a Zero Trust approach, MFA alone is not enough. We must layer in contextbased policies that take into account user, application, device, location and network context.

These next few steps may seem counterintuitive – you will remove the walls you previously worked hard to build. But do not stress, continue the journey to see how it improves the lives and security for the town's people...

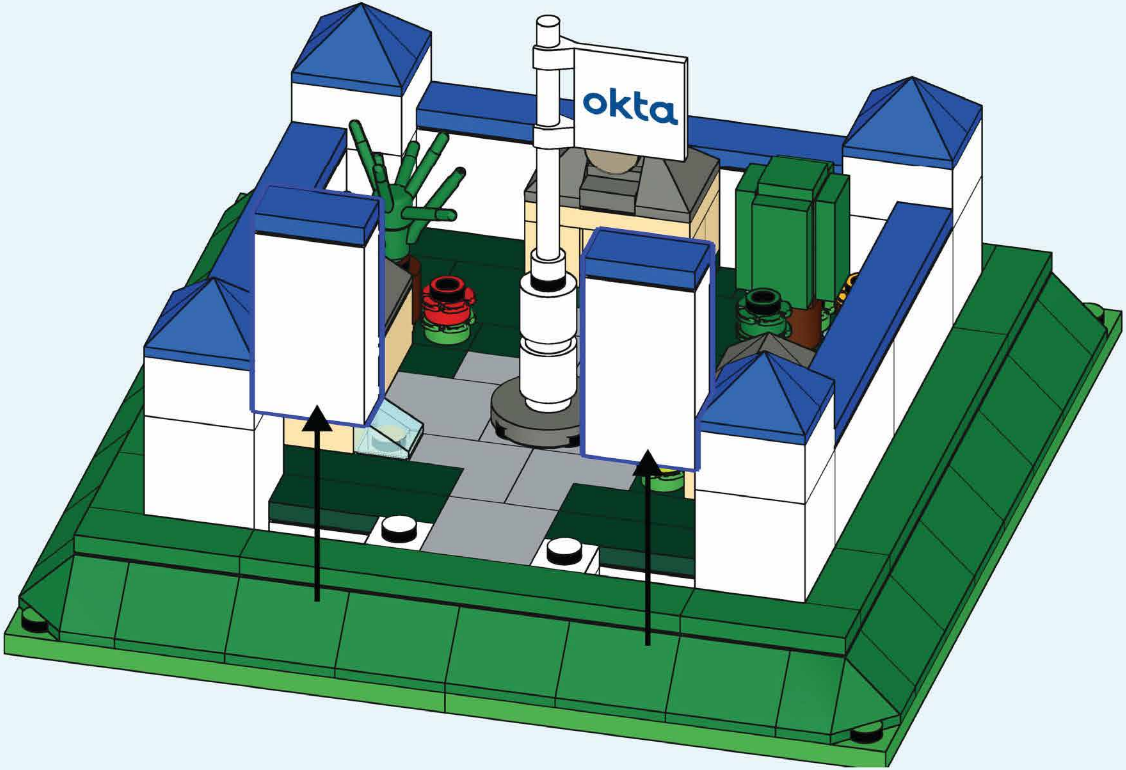
59



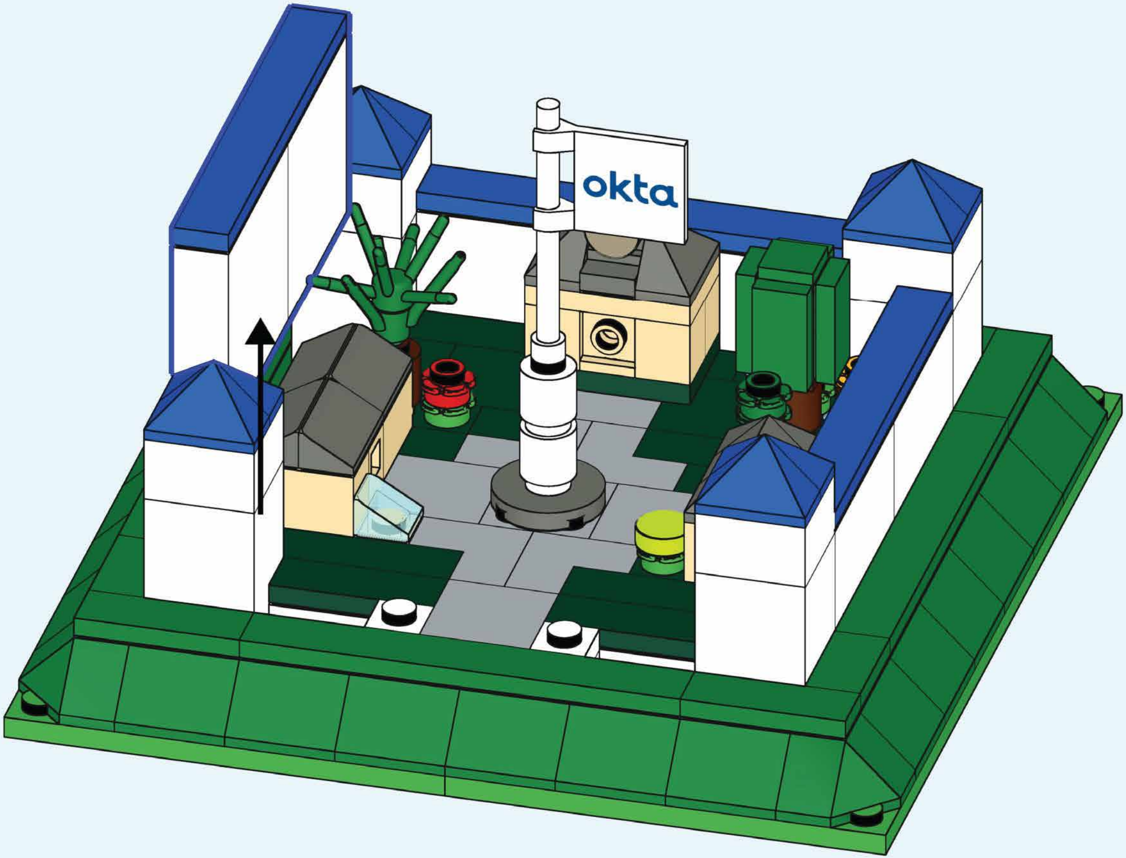
60



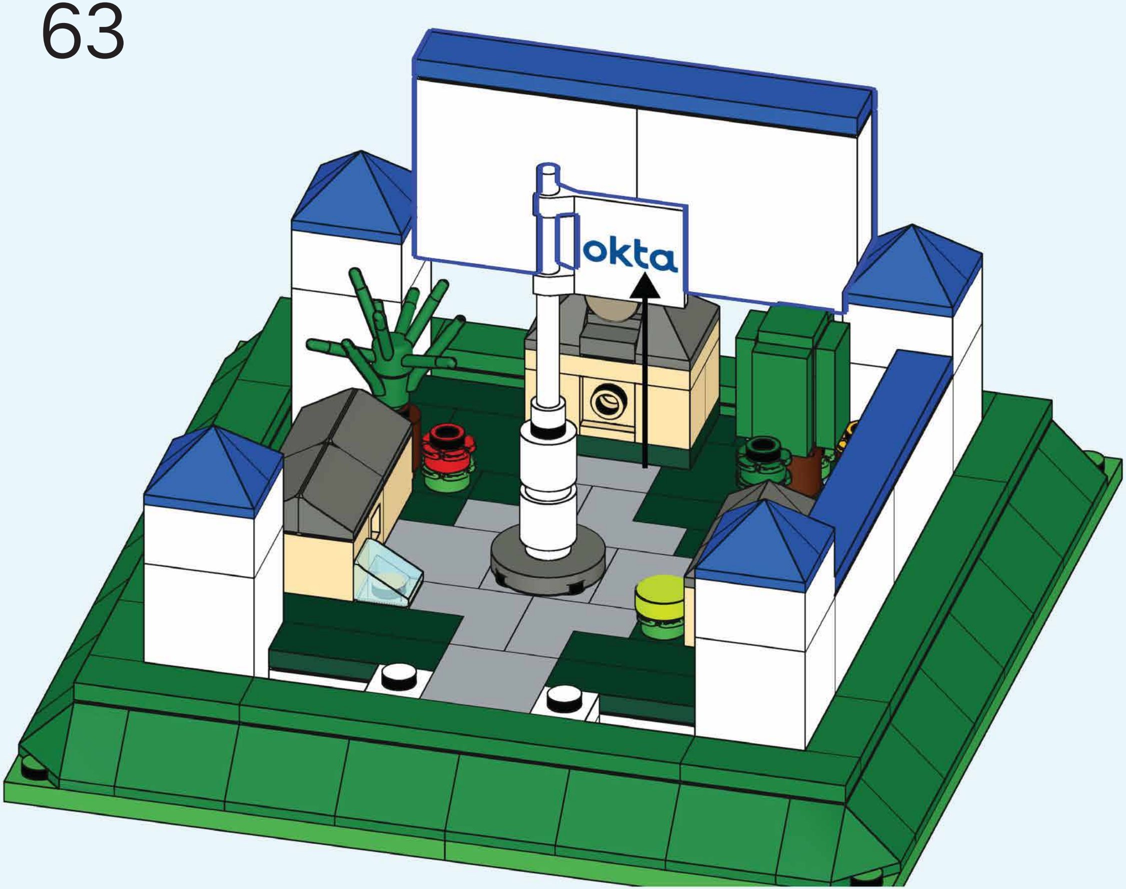
61



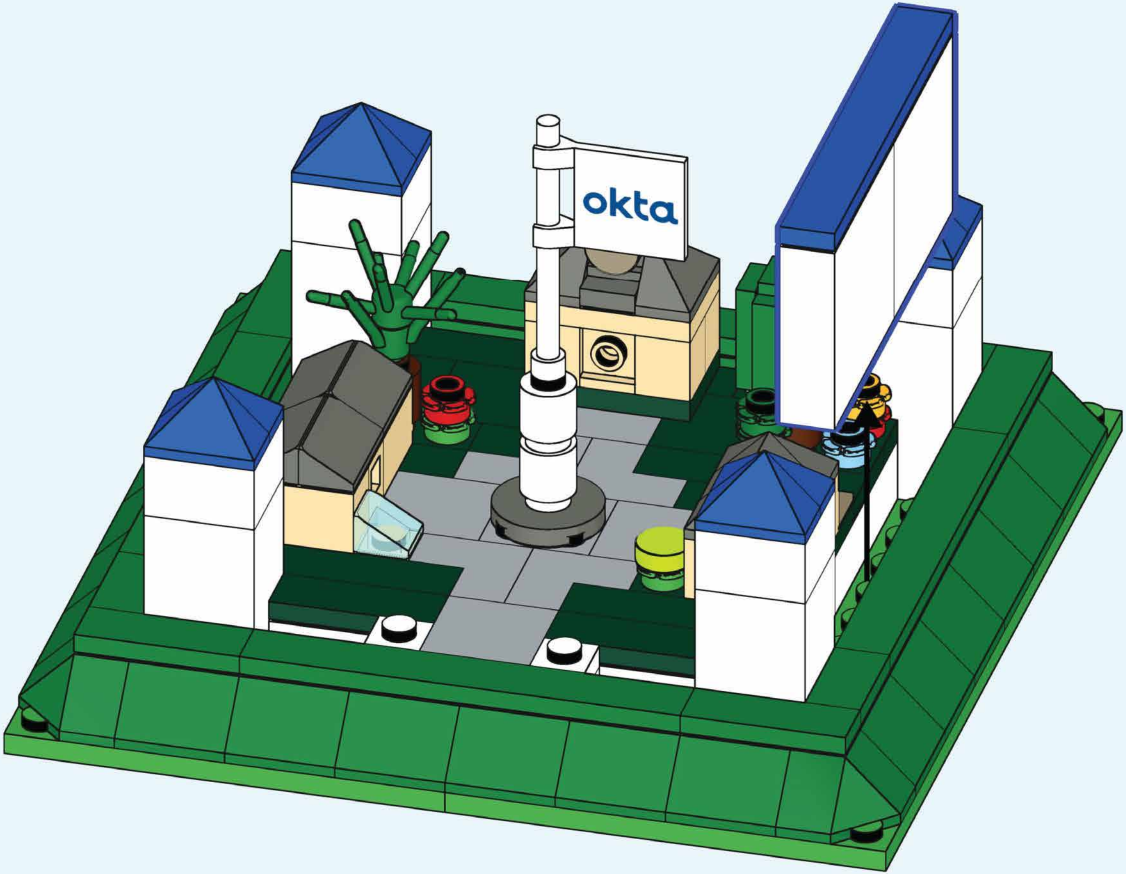
62



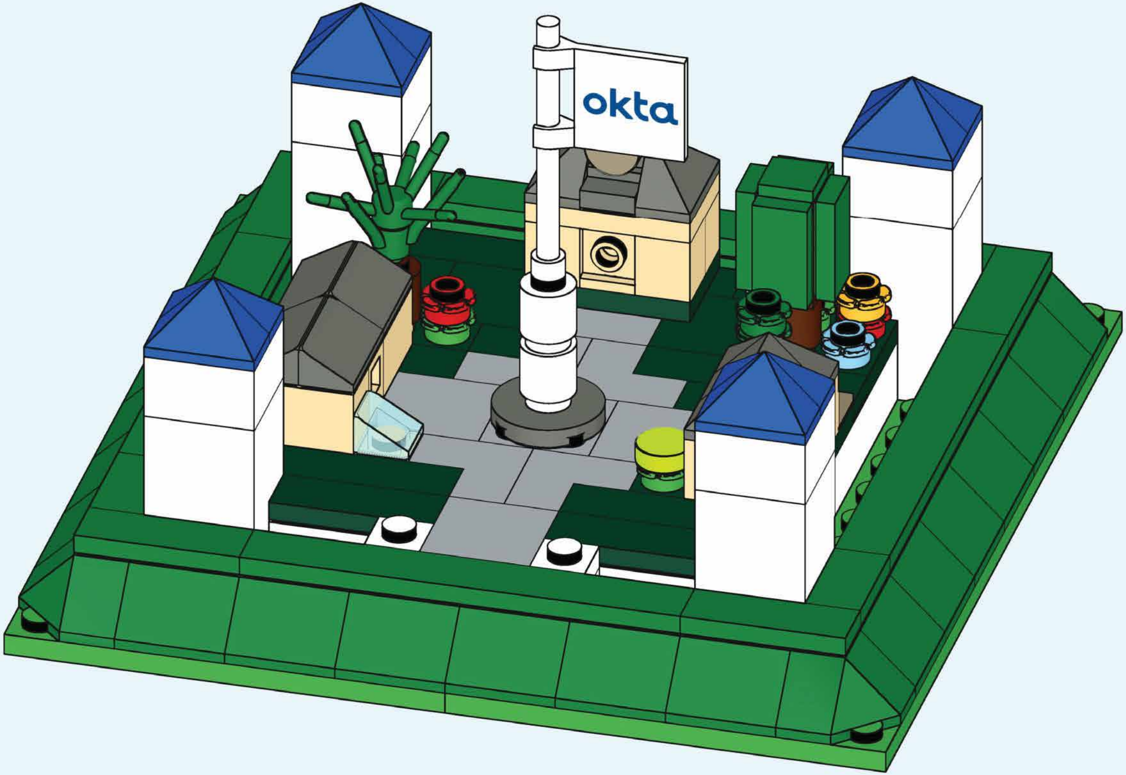
63



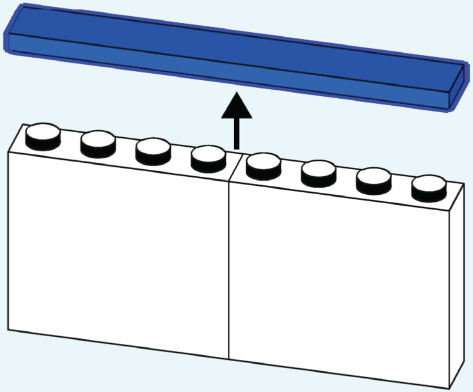
64



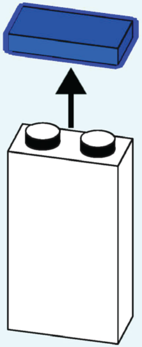
65



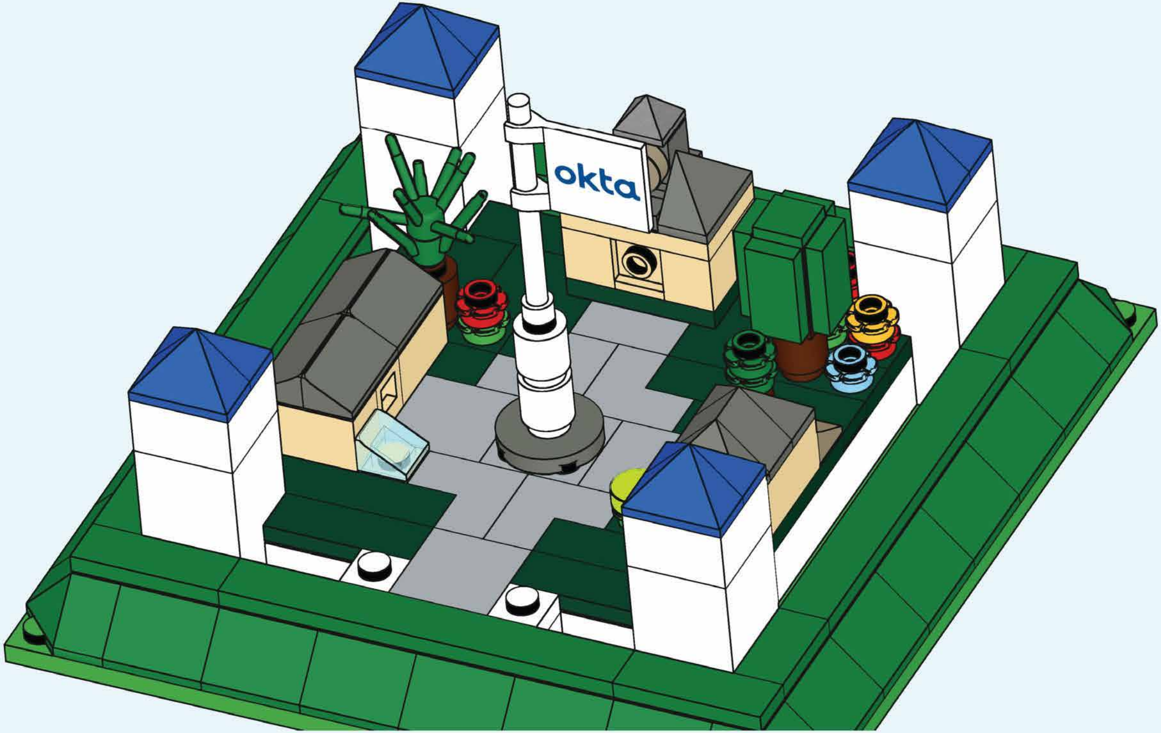
66



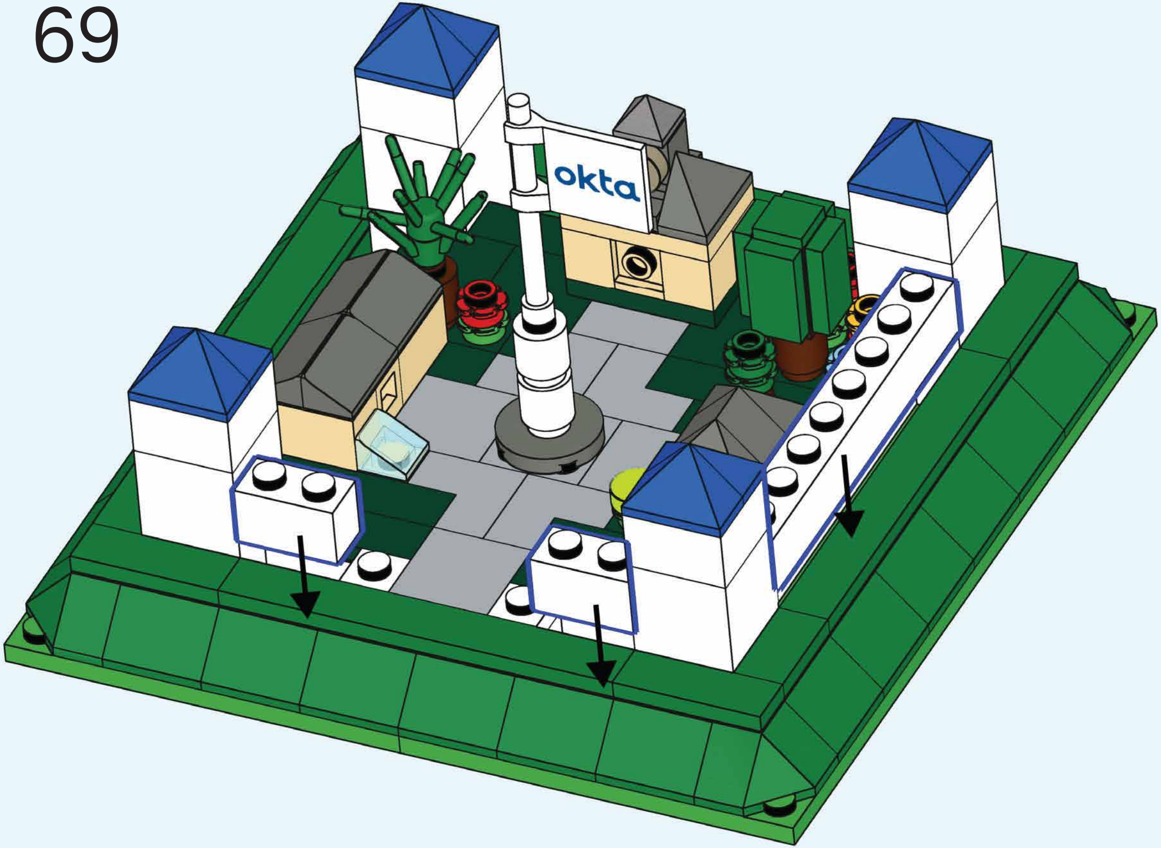
67



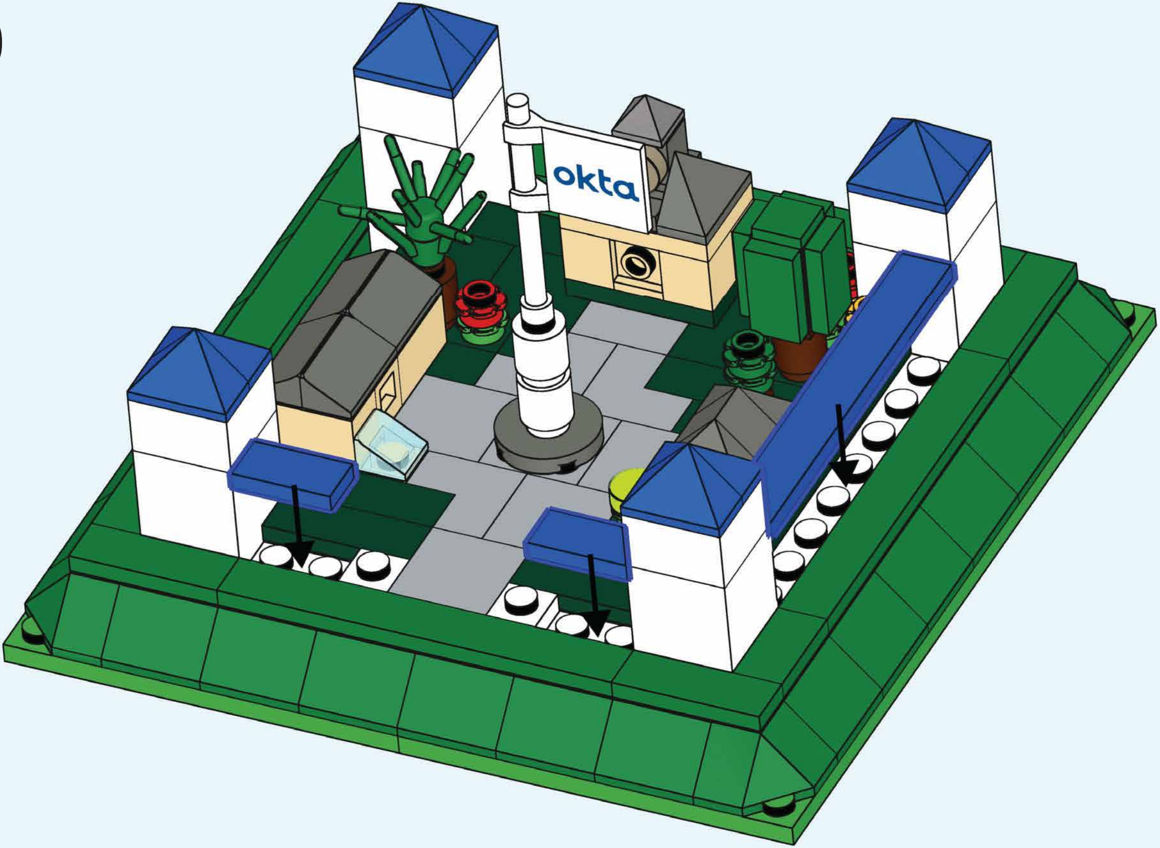
68



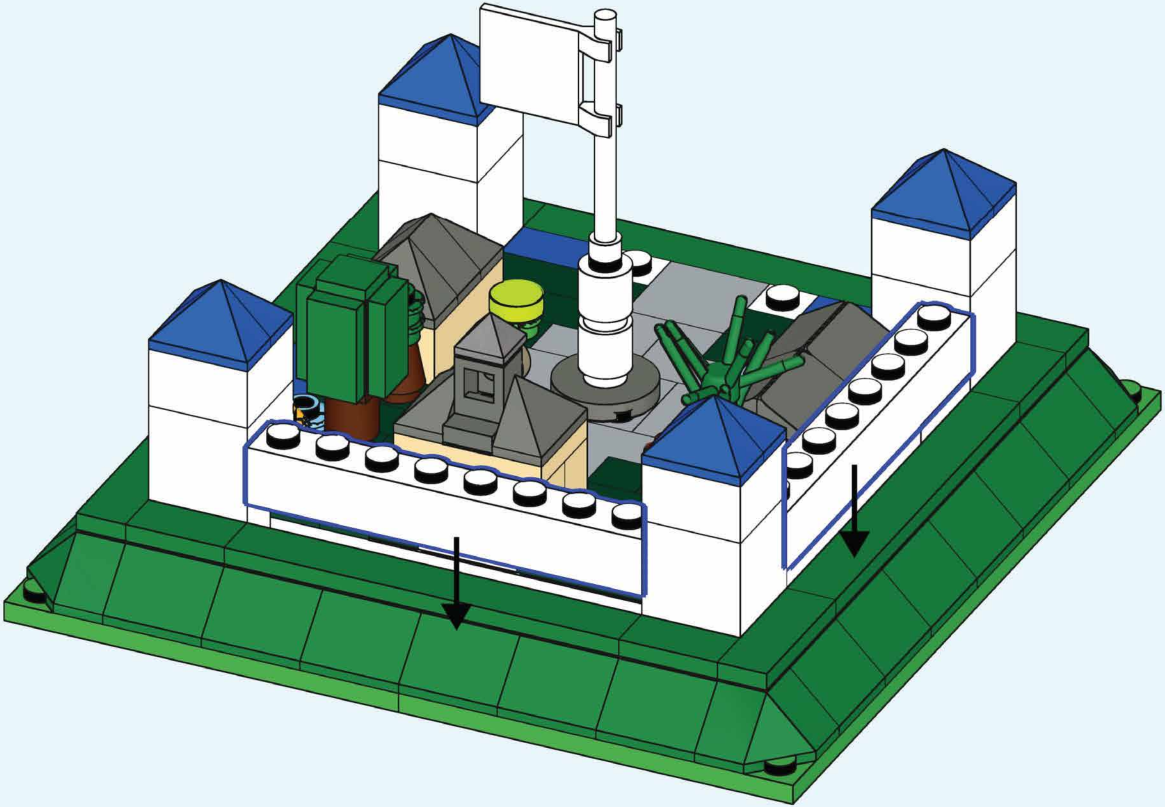
69



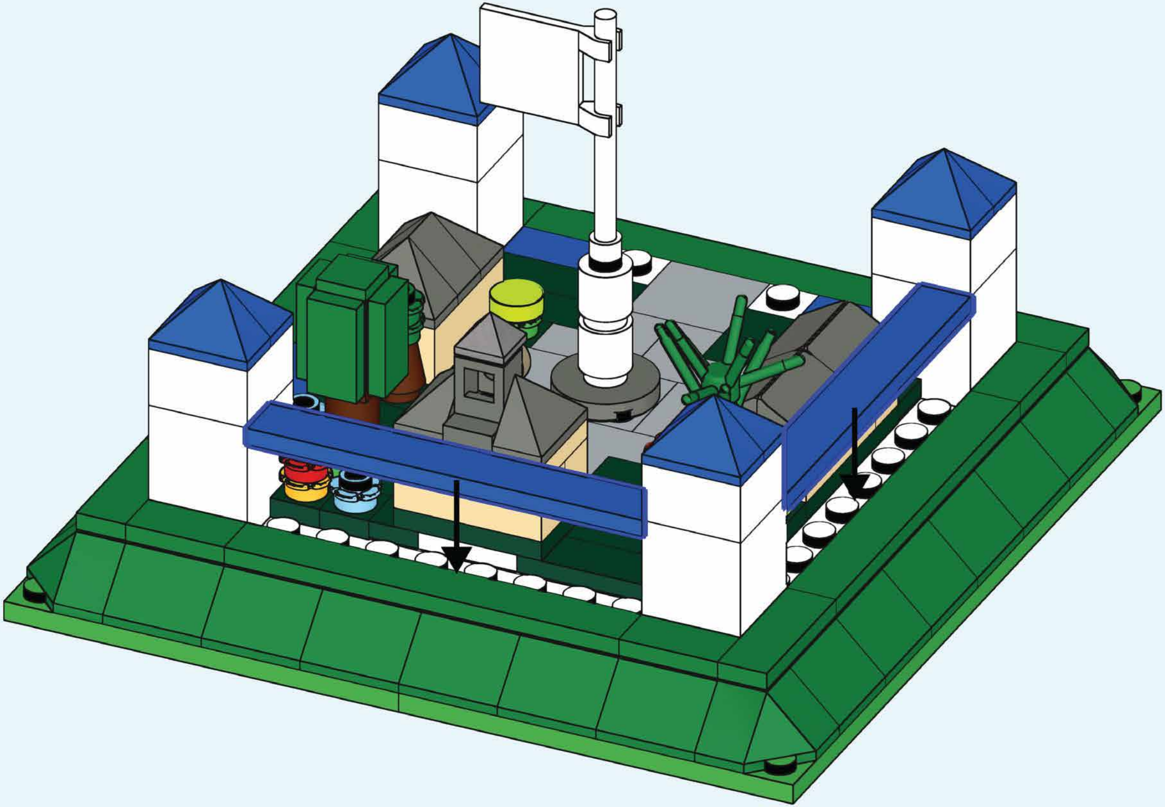
70



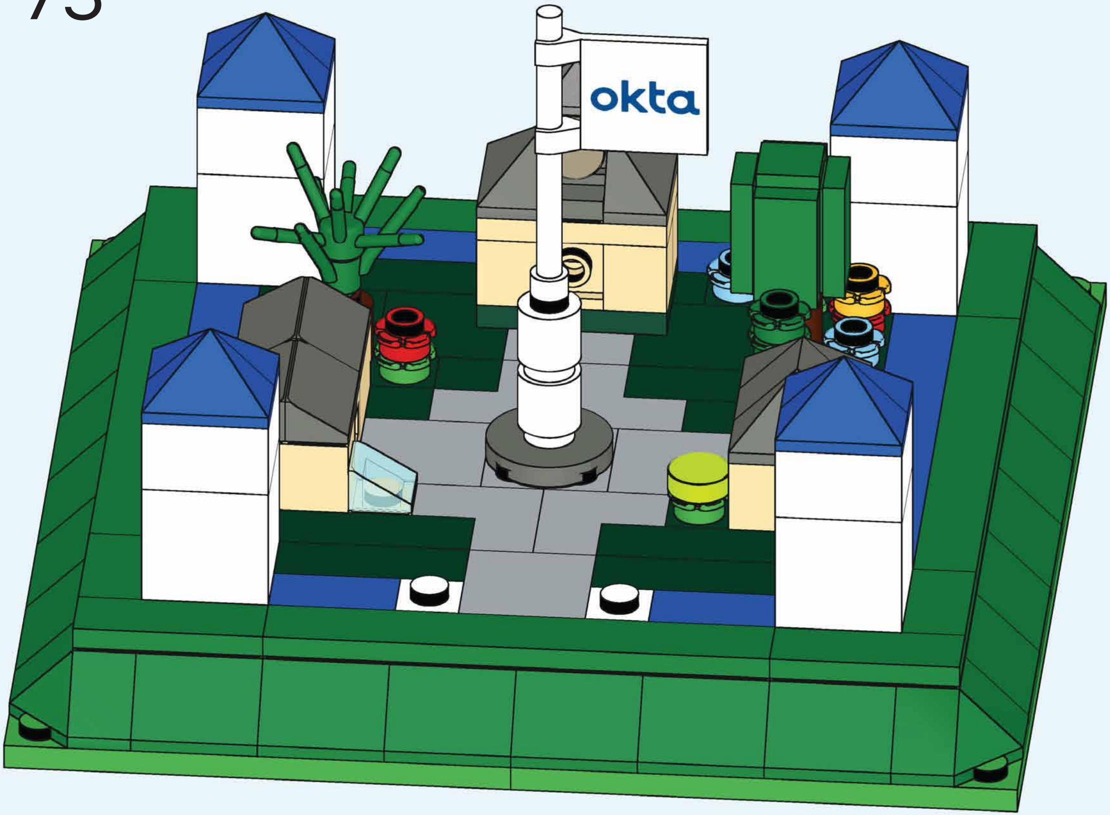
71



72



73



STAGE 3: Adaptive Workforce

Continuous Monitoring, Open and Safe

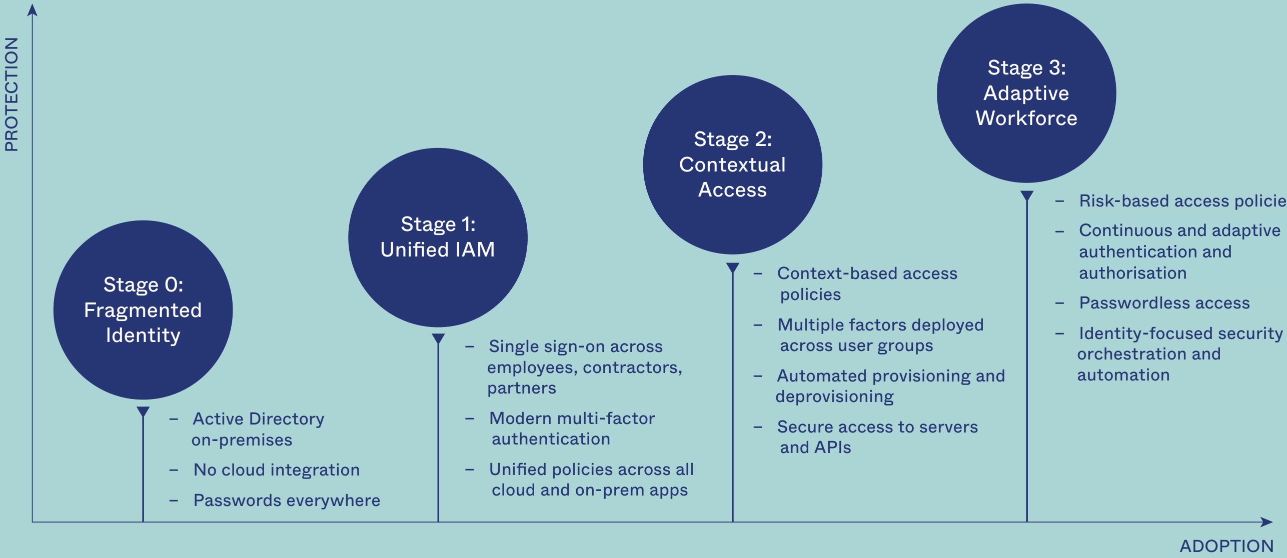
Congratulations, Zero Trust Town has ventured where few towns have! You've recognised that authentication doesn't just happen at the front gate, but continuously throughout the user's experience. It took a leap of faith to remove your walls, but now your towers continuously monitor the town; assessing risk and re-prompting for authentication when it identifies a potential threat. You've made life better for your town's people; they now have frictionless access and don't have to carry a key wherever they go.

In an adaptive workforce, authentication no longer occurs just at entry, but continuously throughout the user's experience. Stage 3 of the Zero Trust journey assesses risk tolerance and uses context signals to determine whether or not to prompt for a second factor. This increases security and simplifies end-user experience, allowing for frictionless access and even passwordless authentication.

okta

Okta and Zero Trust

We recognise that people are the most critical component of the Zero Trust ecosystem. Okta's identity-first approach to Zero Trust security ensure the right people have the right level of access, to the right resources, in the right context, and that access is assessed continuously – all without adding friction to the user.


PROTECTION
ADOPTION
Stage 0: Fragmented Identity
Stage 1: Unified IAM
Stage 2: Contextual Access
Stage 3: Adaptive Workforce

Stage 0: Fragmented Identity

- Active Directory on-premises
- No cloud integration
- Passwords everywhere

Stage 1: Unified IAM

- Single sign-on across employees, contractors, partners
- Modern multi-factor authentication
- Unified policies across all cloud and on-prem apps

Stage 2: Contextual Access

- Context-based access policies
- Multiple factors deployed across user groups
- Automated provisioning and deprovisioning
- Secure access to servers and APIs

Stage 3: Adaptive Workforce

- Risk-based access policies
- Continuous and adaptive authentication and authorisation
- Passwordless access
- Identity-focused security orchestration and automation

Zero Trust Curve

Getting there can be easier said than done, but we’re here to help whether your ‘Zero Trust Town’ is looking to unify IAM, layer in contextual-based policies or level-up to an adaptive workforce.

Learn more at https://regionalevents.okta.com/zero-trust-lego

The right people

Have the right level of access

To the right resources

In the right context

That is assessed continuously

Least Friction Possible