

PROTECT AGAINST OWASP'S TOP 10 IOT THREATS

IoT has emerged as a rapidly growing technology with potential to transform industries, but this growth has also brought with it a host of security challenges and concerns.

WHY THIS IS IMPORTANT?

Given the massive amount of vulnerable IoT devices and server side assets operating in the global economy, we now find critical infrastructure and networks routinely ensnared in the crosshairs of potential cyber-criminals and data thieves. This brief is designed to help manufacturers, developers, and consumers of these devices better understand the security issues associated with IoT, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies.

OWASP TOP 10 IOT VULNERABILITIES

- IOT 01: Weak, Guessable, or Hardcoded Passwords
- IOT 02: Insecure Network Services
- IOT 03: Insecure Ecosystem Interfaces
- IOT 04: Lack of Secure Update Mechanism
- IOT 05: Use of Insecure or Outdated Components
- IOT 06: Insufficient Privacy Protection
- IOT 07: Insecure Data Transfer and Storage
- IOT 08: Lack of Device Management
- IOT 09: Insecure Default Settings
- IOT 10: Lack of Physical Hardening

TRADITIONAL INTERNET SECURITY FAILS TO MEET REQUIREMENTS OF IOT

IoT attacks are growing by 292% and will cost businesses more than \$25 trillion by 2025. The severity of these vulnerabilities is only increased by prevailing myths around IoT security perpetuated by traditional “box and wire” solutions. The biggest misunderstanding is the idea that addressing the broadness of security concerns outlined by OWASP requires a multifaceted approach with a diverse range of makeshift solutions consisting of an assortment of hardware and software products. These solutions only mask an underlying problem - these devices and server side assets remain open to the Internet. The simple truth is: **the only secure port is no port.**

THE CLOUDZITI DIFFERENCE

CloudZiti is the only private, zero trust IoT fabric that allows you to embed security as code and control it from the cloud. The software-only solution protects against the top OWASP IoT vulnerabilities without incurring the expense and complexity of managing obsolete network hardware. This means you can ditch VPNs, private mobile APNs, port forwarding, static IP address reqs, jump servers and bastions, while exceeding US federal zero trust mandates with mutual TLS (mTLS) encryption and X.509 certificate based authentication.



STRENGTHEN & SIMPLIFY SECURITY

Private, zero trust IoT fabric (software defined network) renders all IoT devices and assets invisible to the Internet



REDUCE COMPLEXITY & COST

Simple, software-only solution removes the need to deploy or manage any hardware, replacing truck rolls



SECURE REMOTE MANAGEMENT

Enable simple remote provisioning and management, while eliminating VPN and private mobile APN backhaul



HOW CLOUDZITI ADDRESSES OWASP'S TOP 10 IOT THREATS

Managing IoT deployments with remote management tools made for IT is often clunky. The forced tradeoff between security, simplicity, and performance is often unacceptable. The CloudZiti software platform eliminates the tradeoff and simplifies the deployment by taking care of both remote management and IoT data delivery. The following chart offers a comparison between the effectiveness of traditional solutions (VPNs, private mobile APNs, port forwarding, static IP address reqs, jump servers and bastions) and CloudZiti.

 = competitive advantage




	TRADITIONAL SOLUTIONS	CLOUDZITI ZERO TRUST IOT FABRIC
01: Weak, Guessable, or Hardcoded Passwords Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems	Even if using a private APN managed with a secure mobile VPN (IPSEC), there is nothing to prevent an attacker from accessing the IoT device console or any backdoors if they are listening, and if the attacker can exploit an insecure access point via weak/default credentials. Once on the device, the attacker can see other sensitive data and other devices on the same local network, private APN, or even systems on the internal corporate network that the APN/VPN device is connected to. If servers are only accessible via bastion servers; the security is only as good as the bastion server itself.	CloudZiti makes the device “dark” and eliminates a large portion of this vulnerability by making it almost impossible for an attacker to exploit the system even if there are insecure access points using weak default passwords. If an attacker were somehow able to get on the local network and on the device via an insecure access point using weak/default credentials, the control plane will only allow access to services configured in the policy as opposed to an entire corporate or mobile network. Also, the control plane can monitor the security context for anomalous behavior. 
02: Insecure Network Services Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity, authenticity, or availability of information or allow unauthorized remote control	Even if using a private APN managed with a secure mobile VPN (IPSEC), there is nothing to prevent an attacker from accessing the insecure network services if the device is listening and connecting to the public internet. If an attacker can exploit the device, there is nothing from preventing them from seeing/extracting sensitive data, and to see other devices on the same private APN, the same local network, as well the corporate network that the VPN device is connected to. If servers are only accessible via bastion servers; the security is only as good as the bastion server itself.	CloudZiti makes the device “dark” and eliminates a large portion of this vulnerability by making it almost impossible for an attacker to exploit the system even if there are insecure network services on the device. If an attacker were somehow able to get on the local network and on the device via exploiting any insecure network services, the control plane will only allow access to services configured in the policy as opposed to an entire corporate or mobile network. Also, the control plane can monitor the security posture and context for anomalous behavior. 
03: Insecure Ecosystem Interfaces Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering	A VPN or APN connected using an encrypted tunnel to private/mobile networks will only prevent MITM attacks that could capture sensitive data in transit from the insecure interfaces. They do nothing to prevent an attacker from accessing the insecure web/API interfaces if they can get on the local network or if the device is listening/connected to the internet. If devices are only accessible via bastion servers; the security is only as good as the bastion server itself.	CloudZiti makes the device “dark” and eliminates a large portion of this vulnerability by making it almost impossible for an attacker to exploit the system even if there are insecure web interfaces. If an attacker were somehow able to get on the local network and on the device via exploiting any insecure ecosystem interfaces, the control plane will only allow access to services configured in the policy as opposed to an entire corporate or mobile network. Also, the control plane can monitor the security posture and context for anomalous behavior. 

CONTINUED ON NEXT PAGE

 = competitive advantage

	TRADITIONAL SOLUTIONS	CLOUDZITI ZERO TRUST IOT FABRIC
04: Lack of Secure Update Mechanism Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates	VPNs can potentially provide a secure way to pull system updates if the remote repository resides on the corporate network that the device is connected to, otherwise it may be difficult/impossible to pull updates securely without doing a split tunnel to multiple VPN endpoints. It does nothing to enforce firmware validation or to provide notifications of security changes. APNs may be more viable to mitigate this vulnerability if multiple private APNs can be configured on the device. If devices are only accessible via bastion servers; the security is only as good as the bastion server itself.	CloudZiti can provide a safe and secure way for the IoT device to call the backend update service to pull updates in order to stay current when the update service can be put behind Ziti. 
05: Use of Insecure or Outdated Components Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain	VPNs and APNs do nothing to mitigate these types of vulnerabilities if an attacker can get on the local network and on the device via exploiting an insecure open source component or library. Jump servers and bastion hosts do nothing to mitigate this issue other than to provide some security preventing access to the local network.	CloudZiti makes the device “dark” and eliminates some of this vulnerability by making it almost impossible for an attacker to exploit the device even if it is not patched/updated. If an attacker were able to get on the local network and on the device by exploiting an insecure library or service, the control plane will only allow access to services configured in the policy as opposed to an entire corporate or mobile network. Also, the control plane will monitor the security context for anomalous behavior. 
06: Insufficient Privacy Protection User’s personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission	VPNs and APNs effectively do nothing to mitigate these types of vulnerabilities if an attacker can get on the local network and on the device via exploiting an insecure open source component or library. Jump servers and bastion hosts do nothing to mitigate this issue other than to provide some security preventing access to the local network.	CloudZiti makes the device “dark” and eliminates some of this vulnerability by making it almost impossible for an attacker to exploit the device even if it is not patched/updated. If an attacker were able to get on the local network and on the device, it limits the blast radius of where the data can be sent via the control plane and policy. 
07: Insecure Data Transfer and Storage Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing	VPNs and private APNs can provide security for any data in transit by sending over an encrypted tunnel, but does nothing to mitigate the security of data at rest on the local system if an attacker can get on the device where the unsecured data resides. Jump servers and bastion hosts do nothing to mitigate this issue if an attacker were able to get on the local network and only provide some security accessing the local network.	While enforcing broken access control is an internal security posture, CloudZiti can provide superior security transmitting secure data over its private IoT fabric when the remote services can be put behind Ziti as well. If the device or devices storing sensitive data are secured with CloudZiti it can eliminate some of this vulnerability by making it almost impossible for an attacker to access the data. 

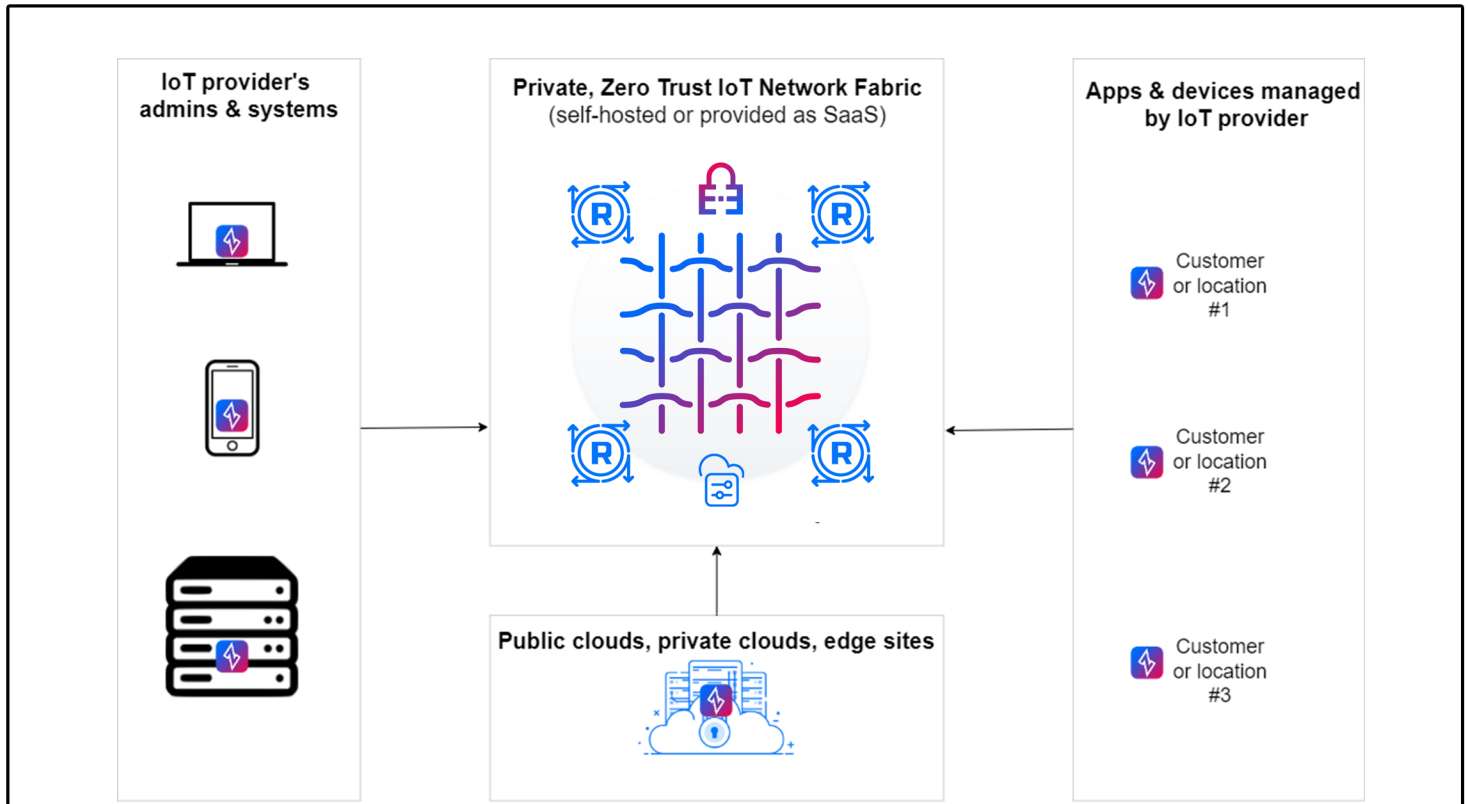
 = competitive advantage

	TRADITIONAL SOLUTIONS	CLOUDZITI ZERO TRUST IOT FABRIC
08: Lack of Device Management Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities	VPNs and APNs do nothing to mitigate the lifecycle of the devices and can only provide secure communication from the device to any external update/provisioning systems on the remote corporate network. Jump servers and bastion hosts do nothing to mitigate this issue if an attacker were able to get on the local network and only provide some security accessing the local network.	CloudZiti provides a secure mechanism for provisioning and updating systems to transmit data to and from the devices, and as always, to make it very hard for an attacker to be able to exploit the device in the first place once plugged into the secure network. It does not enforce or manage the lifecycle and provisioning or deprovisioning of the devices themselves. 
09: Insecure Default Settings Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.	VPNs and APNs do nothing to mitigate the security configuration if an attacker can get on the device. This needs to be prevented by properly hardening the device. Jump servers and bastion hosts do nothing to mitigate this issue if an attacker were able to get on the local network and only provide some security accessing the local network.	If all IoT devices in the ecosystem are secured with CloudZiti, then this will effectively neutralize an attacker from accessing the devices if they were to access the local network. CloudZiti does not mitigate this issue if an attacker can get on the device. This needs to be prevented by properly hardening the device and its security configuration. As always, if an attacker were able to get on the local network and on the device via an unpatched access point, the control plane will only allow access to services configured in the policy as opposed to an entire corporate or mobile network. The control plane can also monitor the security context for anomalous behavior. 
10: Lack of Physical Hardening Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attacks or take local control of the device.	VPNs and APNs do nothing to mitigate a lack of physical hardening on the device if an attacker can get on the device. Jump servers and bastion hosts do nothing to mitigate this issue if an attacker were able to get on the local network and/or device and only provide some security accessing the local network.	If all IoT devices in the ecosystem are secured with CloudZiti, then this will effectively neutralize an attacker from accessing the devices if they were to access the local network. CloudZiti does not mitigate a lack of physical hardening if an attacker can get on the device. This needs to be prevented by properly hardening the device and its security configuration. As always, if an attacker were able to get on the local network and on the device via an unpatched access point, the control plane will only allow access to services configured in the policy as opposed to an entire corporate or mobile network. The control plane can also monitor the security posture and context for anomalous behavior. 

CONTINUED ON NEXT PAGE

CLOUDZITI SOLUTION ARCHITECTURE

The NetFoundry CloudZiti platform is a software-only platform, which enables secure networking for remote management and data connectivity. Private, zero trust network overlays are created which meet and exceed NIST cybersecurity guidelines, while providing high performance. The basic architecture is illustrated below.



- Used for IoT and IT apps, APIs, and devices. All protocols supported, including RDP and SSH. Mutual TLS (mTLS) with all data encrypted. Exceeds U.S. government NIST zero trust guidelines
- Ziti software is embedded in an API or app (agentless), used as a device agent, or gateway. IP address overlap, changes or new sites are non-events. X.509 certs replace need for static private IPs and port forwarding
- Fabric can be extended to any edge to optimize latency and avoid backhaul. Fabric functions as a distributed mesh to optimize availability and resiliency, with dynamic best path routing

GET STARTED TODAY FOR FREE

ABOUT NETFOUNDRY

NetFoundry delivers the CloudZiti private IoT fabric – the world's first programmable, cloud native, zero trust network with near unlimited scale, concurrency, and performance. CloudZiti enables organizations to integrate IoT management, security, and networking as part of a simple solution, and control it from the cloud. NetFoundry transforms secure networking into a developer platform and provides the flexibility of SaaS and open source options.