
GUARDIANS OF GLOCO

Network Security for IoT Devices

12.9.2020

I.T. Security Team (Team 3)

Irfan Malik
Deloran Lyles
Larry Martin
Joe Hines
Benjamin Williams

Executive Summary

Introduction to Gloco

Gloco, Inc. offers eCommerce, content management, marketing, advertising, inventory and customer management solutions, powering some of the most recognizable brands. Total sales on the platform exceeded \$5 billion in 2019 and generated nearly half a trillion marketing impressions. Gloco employs over 10,000 people across 20 offices in North America.

Introduction to the I.T. Security Team

Gloco's Chief Digital Information Officer (CDIO) has tasked the I.T. Security team to assess internal network risks and to provide a solution that increases security, while still providing flexibility. In modern day work environments, that flexibility is required to accommodate the desires of contemporary users--they want to use the same devices they use at home in the workplace. Whether they want to listen to music, have a fun distraction during their lunch break, or even monitor their own home networks, users are adding these IoT devices to enterprise networks. These devices, while convenient for users, pose a significant risk to the enterprise network.

Introduction into IoT Devices

Gartner projects by 2020 21 billion IoT devices will have access to an enterprise network. Historically, IoT devices were novel devices that were deployed by early adopters or to serve a specific enterprise function such as passively gathering data. Primarily, they were hosted on compartmented networks using proprietary protocols outside of mainstream networks. Many devices were designed with no forethought into maintenance or security. They were simply deployed and forgotten.

Now, as adoption of IoT devices has become more widespread, users have brought them onto enterprise networks without recognizing the threats they introduce. In fact, considering that many IoT device manufacturers have yet to integrate customary security practices such as periodic patching and firmware updates, it's apparent that vendors themselves have yet to prepare these devices for enterprise security requirements.

IoT Devices found in our environment can be classified into the following categories:

Smart Speakers

Google Home, Amazon Echo

SmartTVs

AppleTV, FireTV, Roku, Xbox, Playstation, Nintendo

Device hubs

Hue, SmartThings, Hubitat, Lightify, IKEA TRÅDFRI

Typically creates a Personal Area Networks (PAN) that devices connect to using protocols including Zwave, Zigbee, and Bluetooth. The hub will connect to the local network and internet.

Single board computer (SBC)

Raspberry Pi, NodeMCU, Ardrino, WiFi Switches (Tasmota, Govee)

Typically uses WiFi or Ethernet and connects to local network

The approach to solving the problem

Users cannot be allowed to connect unregulated devices onto the enterprise network. Therefore, when new IoT devices are added, they will be restricted from internet and network access. After ownership is identified, it will be assigned to the appropriate network based on the type of device. Further, the device will be fingerprinted based on known identifiers such as MAC address, packet headers and ports used. While on the network, devices will be scanned for out-of-date software, known exploits, or undesirable network performance. If any threats or vulnerabilities are detected, the device will automatically be reassigned to a limited access network and the security team will be alerted.

The integrated solution will:

- Provide Network Access Control (NAC) for authenticating and authorizing devices.
- Manage device's network and internet access.
- Establish a system to fingerprint devices.
- Integrate a vulnerability management system to scan for known threats.
- Perform deep packet inspection.
- Include the ability to check devices for current software and firmware.

A Personal Area Network (PAN) requires a hub to connect to the network which will be covered under the proposed solution. Monitoring PAN devices outside of the hub is out of scope for this project.

Business Context

This is a problem...today

Having a secure network is paramount to delivering a business solution to our customers as well as creating a positive employee experience. The rise of IoT devices introduces new security risks to the Gluco enterprise network. During a recent annual internal audit, several non-managed IoT networked devices were found:

- 3 x Raspberry Pis
- 4 x Amazon Echo- Smart Speakers
- 23 x SmartTVs/FireTV/Apple TVs/Gaming Consoles

During a visual walkthrough of the office, these devices were found in dozens of locations including the employee break room, common areas, and office cubicles. Shockingly, 77% of the devices installed were not upgraded with the latest security updates and 33% had known software vulnerabilities with available exploits. These devices were connected to the network without any security checks or accepting any type of user terms and conditions.

In our current state we would only be able to find these security gaps during the yearly audit. Once discovered these devices would need to be manually updated. If no update or patch is available, then we would not allow these IoT devices on the network. It's important to have visibility into these devices in real time for us to update with a patch or isolate from the rest of the network.

Employees use these devices for collaboration, presentations, side projects, as well as recreation. Raspberry Pi's are popular with engineers and data analysts for creating analytics dashboards and were featured in the company's latest hackathon. Employee's often use Amazon Echo's to facilitate tasks such as setting up calendar invites, reordering supplies, and as a periodic timer in meeting rooms. SmartTVs are used to stream presentations and training sessions. Almost every break room features a gaming console such as an Xbox 1 or Nintendo Switch for employee recreation. Last year Gluco hosted an employee eGaming event for charity. It's important for employees and teams that Gluco can support these devices on its network.

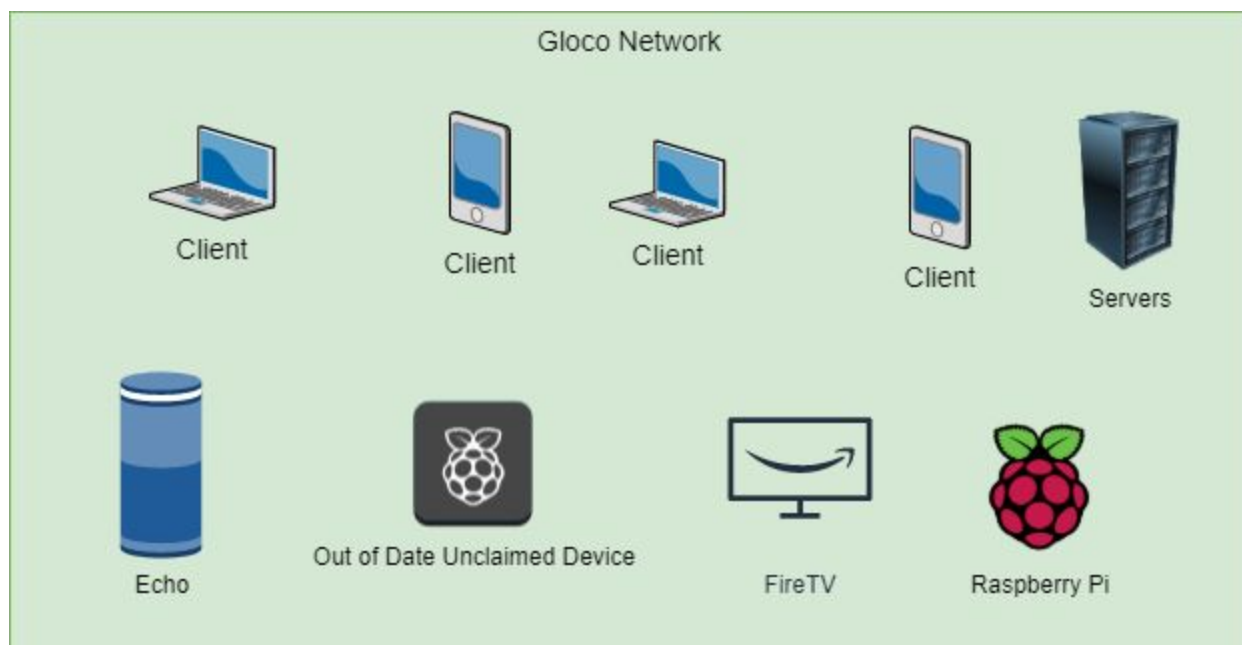
On average a typical employee now uses more than two IoT devices per week. Organizations believe they lack visibility into 40% of end-user devices and organizations with visibility gaps experience 2.3x more security incidents than those without¹. 97% of

¹ Gruber, Dave. Axonius, 2020, *2020 Asset Management Trends: As IT Complexity Increases, Visibility Plummet*s, www.axonius.com/resources/2020-asset-management-trends-report/.

companies have security concerns when adopting IoT, with data privacy being the most important (47%), followed by network-level security (43%), and by device track & management and endpoint security (38%)².

As Is

In the current state users can connect their personal devices to the enterprise network. Even though we have a Network Access Control (NAC) solution, in form of Zones, in place the policies are really relaxed which allows the users to bring in any device and connect it to the same network where all the users reside. This is a huge security risk as we don't know what is on our network and IoT devices may be vulnerable to attacks, infected with viruses or malware which in turn they can pass on to corporate devices.

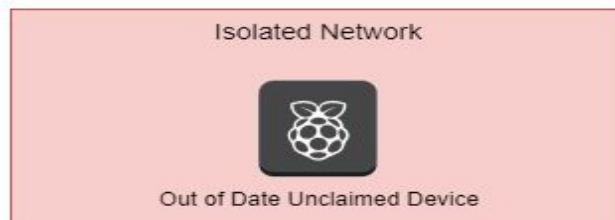
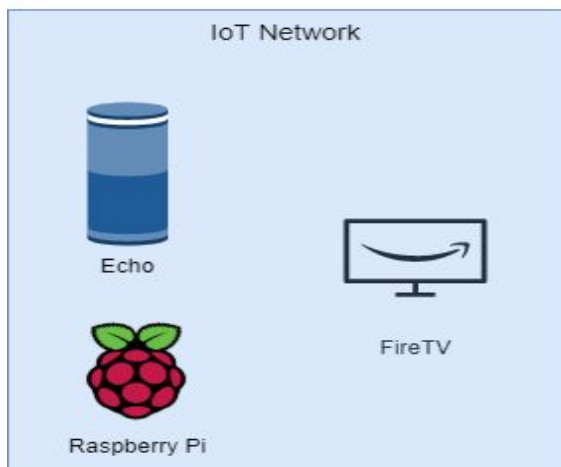


Future State

In the future state the NAC will authenticate every device that is being connected to the network and includes IoT devices. After a user plugs the device into the network or connects it to WiFi the device will be checked against a central database if the device is not found in the database it will be put in an internet only zone (yellow) . At this point users will have 72 hours to claim and update the device or it will move to the quarantine zone (red). On the internet only zone the devices are scanned for vulnerabilities and are allowed to connect to the internet but are not allowed to talk to each other. After scanning if the device is given a

² Microsoft. Microsoft Azure, 2020, *IoT Signals*, azure.microsoft.com/en-us/iot/signals.

clean bill of health it will be put in the IoT network zone (blue) which will allow some communication between the users that are on the enterprise network (green) to these IoT devices and IoT devices will be able to communicate with each other as well.



Required Functionality

For our internal tools to successfully identify an IoT device and prevent potential breach scenarios, we will incorporate several specific features into our proposed solution. The required functionality can be broken down into two categories. The adding and usage of the IoT devices, and the security of Gloco's network.

Functionality for the security of Gloco's network

Feature: Only allow authorized device to connect to the network

Benefit:

Full awareness of devices connected to the network provides protection against threats. Before we can stop what's out there, we must know what is running out there. We will allow users to use IoT devices, but we must take precautions to protect our network, our intellectual property, our clients, and our data. Knowing what devices are connected to the network will allow easier audits.

User Stories:

As a User, I want a streamlined IoT device authorization process, so I can add new devices to the network to enhance my work experience. The process needs to be easy so that non-experts can do it without cumbersome instructions or extended wait times.

As a User, I am required to fill out a form before my IoT device can connect to the network.

As a Security Analyst, I want to know what devices are connected to the network and who owns them so I can immediately remove unauthorized hardware.

As a Security Analyst, I want to be alerted when an IoT device joins the network, so I have a record of all devices.

As a Stakeholder, I want to have a secure network and only allow devices that are being used.

Acceptance Criteria:

- Have a policy in place that requires users to keep devices updated and to consent to having a device removed without warning if the security analysts deem it a threat
- A system that will prevent unauthorized devices from connecting to the network.

-
- The system will allow devices to connect to the network in a restricted access space, so a user can have it authorized.
 - The ability to send alerts and generate reports on network connected devices.

Feature: Detect and Identify devices on the network

Benefit:

In order to properly protect the network, we need to know what is on our network and what level of access the device or user has. This also helps us in situations where users are bringing in unpatched and unknown devices, putting them on our network and giving hackers an easy target.

User Stories:

As a Security Analyst, I want to easily detect, record and manage any device connected to the Gluco enterprise network, so I can protect the network from attacks.

As a Security Analyst, to be able to determine what the device is through multiple detection schemes, so I know the device is what it says it is.

As a Stakeholder, I want to get a list of all IoT connected devices, so I can conduct accountability audits.

Acceptance Criteria:

- The ability to detect devices and identify the type of device.
- Alerting method when device joins the network,
- The use of multiple techniques of detecting a device to create a fingerprint.
- The ability to generate reports.

Feature: Continuous scan of networked devices for vulnerabilities.

Benefit:

Devices with known vulnerabilities or exploits can open the doors for an attack. By checking for vulnerabilities, isolating at risk devices, and having an updating policy will reduce the attack profile.

User Stories:

As a User, I want to keep my device updated, so I can stay compliant with the company policy.

As a Security Analyst, I want all devices that are connected to be checked for known vulnerabilities, so I can keep the network safe.

As a Security Analyst, if a device is detected with a vulnerability, I want it isolated, so I can protect the device from the vulnerability.

As a Security Analyst and User, if a device is detected with a vulnerability I want to be notified, so I can conduct remediation on the device.

As a Stakeholder, I want all devices to have the latest security patches installed, so there is a reduced risk of an attack.

As a Stakeholder, I want all to be able to report on scan, so I can report out results to outside stakeholders.

Acceptance Criteria:

- System that can scan devices and have a repository of known vulnerabilities.
- Scan devices for vulnerabilities on a regular cadence.
- Devices that have a vulnerability will be put in a Secure Network where they will not be allowed to talk to other devices till the vulnerability has been patched.
- Create a quarterly audit where device owners are required to check devices for latest updates.
- Notification of device vulnerabilities sent to the appropriate people.
- The ability to generate reports on vulnerability scans.

Functionality for the use of IoT Devices

Feature: Be able to utilize the features of Alexa and other smart voice control hubs

Benefit:

Alexa and other voice control devices can convert voice to digital interactions such as turning on a light bulb in the office, making a checklist, creating reminders, and scheduling meetings.

User Stories:

As a User, I want to utilize a network connected smart device, controlled via my voice, so I can save time by not having to physically interact with devices to make them function.

As a User, I want to verbally set a timer, so I can limit the amount of time I spend on an activity.

As a Security Analyst, I want the voice control devices to be separated from the production network and only have access to the internet. The traffic between the Voice HUB and the internet would be monitored and subjected to Deep Packet Scan.

As a Stakeholder, I want to make sure these devices are at a safe physical location where they can't be misused by sniping my voice through a laser³ or by yelling from outside a window or door. If the product offers voice recognition, that feature should be enabled.

Acceptance Criteria:

- Voice hubs can connect to the internet and other smart devices.
- Devices are isolated to a Virtual Network with limited, closely monitored access.
- How and where to place IoT devices locations are defined.

Feature: Able to utilize the features of a SmartTV and other TV connected devices**Benefit:**

SmartTVs have built-in functionality that can be used for entertainment, education and to share content to a group of people.

User Stories:

As a User, I want to utilize a network connected SmartTVs, so I can present clear presentations to stakeholders from my cloud storage and local machine.

As a User, I want to utilize the apps on a SmartTV, so I can stream content from the internet.

As a Security Analyst, I want the SmartTVs isolated from the internal network, so it won't have access to sensitive systems.

As a Security Analyst, I want SmartTVs to be required to obtain recent security updates, so that an attacker does not exploit a known vulnerability.

³ Wired.com, Article "Hackers Can Use Lasers to 'Speak' to Your Amazon Echo or Google" Link Home <https://www.wired.com/story/lasers-hack-amazon-echo-google-home/>

Acceptance Criteria:

- SmartTVs can connect to the internet and stream media.
- SmartTVs can receive content from an individual's laptop.
- If a SmartTV has stopped receiving updates, move it to an isolated network.

Feature: Connect Single Board Computers (SBC) to network**Benefit:**

SBC, like the Raspberry Pi, are cheaper than full computer solutions. In many cases using an SBC can be 90% cheaper and provide the intended functionality. Other types of SBC include WiFi enabled light switches.

User Stories:

As a User, I want a device that can connect to our build agents (SBC connected to LED lights), so I can get immediate feedback on the build status.

As a User, I want to have a Raspberry Pi displaying application status, so I can monitor the health of applications that power Gloco's business.

As a Security Analyst, I want access to SBC, so I can ensure they meet our security standards.

As a Stakeholder, I want to limit the devices which can be properly secured, so I can protect the company from risk.

Acceptance Criteria:

- Device is registered with the security team and they have login credentials.
- Published list of acceptable devices for company procurement
- Devices can connect to the internet and the ability to access other network devices.

Feature: Connect IoT hubs to network**Benefit:**

IoT hubs allow users to control devices that connect to it through a personal area network (PAN). Common use cases include using smart bulbs, like Hue, which are typically maintained by the manufacturer longer than cheap WiFi bulbs. Hubs allow the use of other devices like motion sensors and you can set up events to trigger lighting.

User Stories:

As a User, I want an IoT Hub to power my smart color lighting, so I can control the lights from other network connected devices.

As a Security Analyst, I want IoT hubs to be separate from the main network, so they will not interfere or have access to other devices.

As a Security Analyst, I want IoT hubs to have a secure password and not use a personal account, so that they are less likely to have their password compromised.

Acceptance Criteria:

- Hub is connected to the network, with limited access.
- Hub is accessible to the user so they can access the connected devices.
- Password is stored in a location that only needed people can access and follows Gloco passwords policies.

Business Benefit Justification

Enabling Teams/Improving Employee Experience

Teams will be empowered to use IoT devices to help deliver great products. IoT devices allow the ability to share content, monitor systems and provide needed breaks from the workplace. Teams that have easier time working with technology are higher performing and happier. More importantly, having the ability to use IoT devices increases employee engagement. Companies that were early to adopt IoT in the workplace report an increase in collaboration within the business, market insight, and employee productivity⁴. A recent survey for Gloco showed that over 60% of employees believed that using IoT devices made them more productive and increased satisfaction.

Increased Accountability of Devices

Implementing the IoT device program will require some administrative overhead for our team at Gloco. If users decide to add an Alexa or other IoT device to the network, they will be required to accept the terms and conditions and fill out the following information: *First Name, Last Name, Employee ID, Email, Department, Device Location, Asset Tag, Mac Address*

⁴ Harvard Business Review Analytic Services. Verizon, 2014, *Internet of Things: Science Fiction or Business Fact?*, hbr.org/resources/pdfs/comm/verizon/18980_HBR_Verizon_IoT_Nov_14.pdf.

With this information we can quickly identify owners of devices. Currently when an unknown device is detected it takes on average a 20 hours of effort to identify the owner, often resorting to a security analyst walking around looking for the device. With the proposed solution this will be automatic and require no additional hours of effort.

Reduced Overhead/Faster Remediation

Device updating and remediation is being done ad-hoc and manually. Many devices are only being updated after the yearly internal audits and some devices may never be updated. During the audit only 33% of devices were up to date in their patches. In future audits we want this number to be as close to 100% as possible.

The yearly audit is time intensive and requires many reports to be created manually. Last year's audit and remediation took over a month. This included approximately 1,000 hours from the security and network teams. It is estimated that having the solutions in place can reduce the audits down to a few days and less than 40 hours of effort. This effort could lead to a potential 90% reduction in costs, while freeing time for other important activities and allowing for more frequent automated audits.

Managing Risk

The average cost of a data breach for a 10,000 person company is almost \$4 million⁵. A breach is also subject to potential fines for PCI compliance. A high profile breach could cost hundreds of millions of dollars in lost revenue due to client churn. Overall impacts on the business include losses in data, operations/productivity, as well as confidence with our customers. Data loss and breach of confidentiality such as PII can also lead to potential lawsuits. Companies that invest in a comprehensive incident response plan save over \$1.2 million⁶ a year on potential security breaches than ones who do not.

Our business is built on trust, with both our clients and client's customers. Clients trust that we are securing their data and their customers trust that we have secured transactions and protecting their personal identifying information. A preventable data breach will cause loss of trust and cause clients to look for alternative solutions. Having a known security breach will make it difficult to attract new clients and prevent us from growing our business.

⁵ Ponemon Institute. IBM, 2019, *Cost of a Data Breach Report*, www.ibm.com/security/data-breach.

⁶ Ponemon Institute. IBM, 2019, *Cost of a Data Breach Report*, www.ibm.com/security/data-breach.

PART 2. TECHNICAL SPECIFICATIONS AND PROTOTYPE

Architectural approach

Gloco's I.T. Security has broken down the need into the following four categories:

1. A way to discover and identify IoT devices (Fingerprinting)
2. The ability to segment IoT devices based on required level of access
3. A system to scan devices for vulnerabilities
4. The ability for devices to be assigned to users

The following existing Gloco platforms will be leveraged:

- Palo Alto Networks for Next Generation Firewall segmentation
- Rapid7 InsightVM for vulnerability scanning
- Palo Alto for Device Identification
- Splunk for log aggregation and reporting
- Okta for Single Sign On, authentication and account status
- AWS for hosting the IoT Device Management Portal



Software Solution

Gloco is a large organization with a robust network⁷ that is deployed to over twenty locations and includes over 15,000 networked devices. The majority of the devices are employee laptops and workstations, managed phones and tablets, and servers both in the cloud and on site. Over the last few years we have expanded our platforms to include robust industry leading solutions in the networking and security vulnerability scanning space. These platform solutions have been solely focused on the standard corporate issued networked devices, and were not set up to adequately handle the rise of IoT devices joining Gloco's network. Many of our vendors have started to roll out IoT specific functionality into their platforms, allowing proper management of the entire network. When evaluating the needs of this project we looked at the existing platforms and compared them to other solutions.

Palo Alto

Current

During FY2019 Gloco invested in moving to Palo Alto's Software Defined Wide Area Network (SD-WAN) solution. This enabled intelligent routing of network and internet traffic from Gloco's office locations across the country. Leveraging SD-WANs Gloco has the ability to route traffic through optimal channels and remove unnecessary routing.

Proposed

Gloco is currently using the Palo Alto Networks Security Operating Platform in a limited capacity. The current architecture does not account for our zone-segmentation solution to isolate IoT devices. All IoT devices and users are currently positioned in the same zone. This limits our IT Security team's ability to properly secure our enterprise network from new and emerging threats. We have limited, best-effort ability to identify network applications by using the Server Name Indication (SNI). While this method gives us an idea of what we may have on our network, we would like to leverage the full functionality of our Security Operating Platform. This will give us true network visibility.

We will decrypt traffic where appropriate. This will allow our team to perform a true Deep Packet Inspection (DPI). We will use this functionality along with the platforms Device ID capability to categorize IoT devices and apply our corporate security policy (security rules)

⁷ Network Architecture Diagram can be found in the Appendix

dynamically. Lastly, we will incorporate our newly designed Zone-Based architecture for network segmentation. All Inter-Zone traffic will be blocked by default and will require a security policy to allow any connectivity between zones.

Palo Alto Device-ID⁸

When the user connects her consumer IoT device to the network, the Security Operating Platform provided by Palo Alto Networks Device-ID will fingerprint the device and assign it into the appropriate zone. That action generates a security event in the network device log files.

Palo Alto Next Generation Firewall (NGFW)⁹

Using Palo Alto Next Generation Firewall, we will segment Gloco network into the following four zones:

GREEN ZONE - Gloco's managed corporate devices

- Laptops, Servers, MDM managed devices

BLUE ZONE - Trusted IoT Devices, which will have access to the green zone

- FireTV/AppleTV that users can stream content from their corporate laptop
- Device in green zone can connect to device in blue zone which can communicate between the zones (two-way communication)
- Secure protocols used by trusted IoT devices will be allowed into green zone

YELLOW ZONE - Un-trusted devices, which will have limited access to the green zone

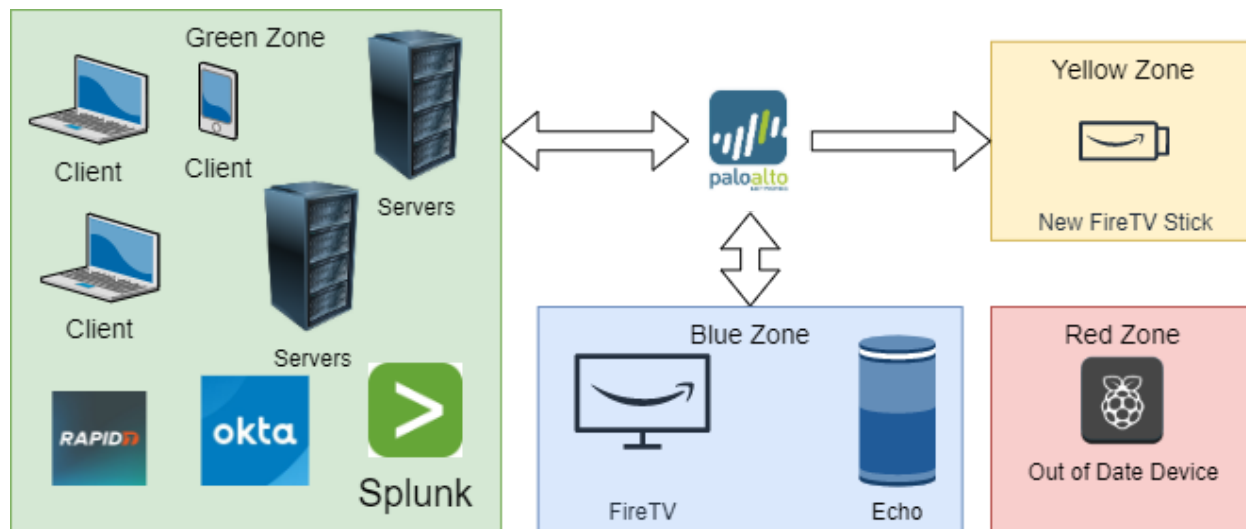
- New device that needs to be owned or a device that falls out of compliance
- Any device in the yellow zone for 72 hours will be moved to the red zone
- Yellow zone is restricted to one-way communication from the green zone

RED ZONE - No access to any resources, completely isolated

- Device that is out of compliance and needs to be removed from network

⁸ For Screenshots and Vendor Comparison See Appendix under Palo Alto Solutions

⁹ For Screenshots and Vendor Comparison See Appendix under Palo Alto Solutions



Rapid7 InsightVM

Current

We selected InsightVM because it was an industry leader in vulnerability scanning. The way it is setup right now it does a discovery scan on Monday of every week and finds all the devices that are on the network. Tuesday it runs a vulnerability scan against all those devices and records the results in the Vulnerability Database. The results are then compared against known exploits and reports are generated for the assets that have the highest risk and the Security team generates tickets for appropriate teams to get these vulnerabilities remediated. Depending on the criticality of the vulnerability it can take anywhere from the same day to 30 days to remediate vulnerabilities. The rules are not set up to appropriately classify vulnerabilities in IoT devices.

Proposed

InsightVM will add a new scan schedule for IoT devices. No matter what zone they are in they will be scanned every day. The results are then sent over to Palo Alto which will then take appropriate action depending on the criticality of vulnerability. InsightVM has a scoring system it uses to categorize different vulnerabilities. Palo Alto will use the following chart to make the decision on where to put the devices.

7k-10k+ Risk score = Yellow Zone for 72 hours after which it is moved to Red.

5k - 7k Risk score = Blue Zone for 5 days after which it is moved to Yellow Zone.

1k - 5k Risk score = Blue Zone for 30 days after which it is moved to Yellow Zone.

The devices in the Red zone will require user intervention by the service desk to move back to the yellow zone.

Address	Name	OS	Vulnerabilities	Risk	Last Scan
192.168.222.189		Ubuntu Linux	0 5	39	11,394 Nov 8th, 2020
192.168.222.108	EPSON7F02E7	Epson 11b/g/n Print Server	0 1	21	9,738 Nov 8th, 2020
192.168.222.72	octopi	Raspbian Linux 10.0	0 0	10	4,387 Nov 8th, 2020
192.168.222.1			0 0	11	3,995 Nov 8th, 2020
192.168.222.114		Linux 3.2	0 0	7	2,957 Nov 8th, 2020
192.168.222.76		Nest embedded	0 0	0	0.0 Nov 8th, 2020

Splunk

Throughout the fleet, our infrastructure logs, system hardware logs, application logs, and network device log files are currently monitored by Splunk. With Splunk we have the ability to create reports from logs, generate alerts, and create dashboards. Using dashboards has made monitoring simpler for our security administrator, as it helps ensure that no alerts are overlooked or misclassified. All platforms will generate log files that will be captured in Splunk. Every platform within Splunk will have alerts and reporting setup.

Okta

Gloco leverages many technologies, platforms, and infrastructure throughout the organization. Okta provides a single sign-on and user management solutions. Single sign on makes it simple for our users because no matter what application they access, it authenticates with one account. Okta simplifies managing users and assigning appropriate access.

Okta will be used by the IoT Device Management Portal to identify the logged in user when they are claiming ownership of an IoT device. When an employee leaves Gloco, Okta will notify the other platforms and move any IoT device that was owned by them into the yellow zone.

ServiceNow

ServiceNow is the existing ticketing system that makes it easy to automatically generate service desk tickets based on specific events. Integrations with ServiceNow will be further leveraged to automate the process of handling IoT device issues and notifying the appropriate people. IoT device owners will be responsible for remediating and documenting actions in tickets. The I.T Security team is responsible for the network so the majority of tickets they will be notified on.

Leveraging ServiceNow tickets will allow users to be able to request and manage IoT devices

at Gluco. The self-service process flow will lessen the burden on the I.T. Security team and streamline the device approval and remediation process.

Below is a list of sample events that could trigger ticket creation:

Event	Ticket Sent To	Priority
IoT device joins network	I.T. Security team	2 - High
Critical vulnerability found on IoT device	I.T. Security team, Device owner	1 - Urgent
IoT device owner left company	I.T. Security team, Dept. head	3 - Medium

*This is not a comprehensive list of ticket events

IoT Device Management Portal

Glco Employee User Experience

Users will register their IoT devices in the Gluco IoT Device Management Portal. This is a private portal where users will authenticate with Okta. Once logged in the user will see a list of unregistered IoT Devices types and MAC addresses in the yellow zone. A link is provided that will give users instructions on how to find their specific device's MAC address. Users will then be able to confirm the address against the MAC address listed under the unregistered devices. On the right side of the web page user information will be auto populated from Okta to include: First Name, Last Name, Employee ID, Email, Department. The user will then need to input their Device Location, Device Model, Tag Number and MAC Address. After an employee submits a form their device information along with the zone and last scanned date will be stored in ServiceNow. This information is available only to the Gluco I.T. Security team and will be leveraged for reporting. Once the form is filled out and the IoT device passes a vulnerability scan it will be moved into the blue zone. If the device ever falls out of compliance after approval they will receive an email from ServiceNow notifying them their device was moved to the yellow zone and they have 72 hours to take action or their device will be removed from the network.

UNREGISTERED DEVICES

Note: This is not for laptops or phones. Do not try to connect without registering your device's MAC address first. If you do, your device will not connect successfully.

To Begin: Find your device listed below. You can find the MAC address here: [Find Your Device's MAC Address](#)

Device Model	Mac Address	Zone
Raspberry Pi - Compute Module 4	C0:8F:36:A5:5B:A5	yellow
Play Station 4 Pro	0F:54:0B:B3:DC:5C	yellow
Amazon Echo Show 10 3rd Gen (2020)	32:11:E4:DB:56:A8	yellow
Amazon Echo Dot 4th Gen	22:73:41:A7:41:66	yellow
Nintendo Switch	02:75:81:D4:5B:65	yellow
6000X - 4K Roku TV	8B:F9:E0:DC:22:DB	yellow
Roku Streaming Stick	AB:E7:73:37:5A:DE	yellow
Amazon Echo Dot 4th Gen	8E:C2:DC:D7:7B:EE	yellow
Amazon Echo (2020)	2F:04:07:82:12:A6	yellow
4660X - Roku Ultra	2A:A8:50:90:CF:BD	yellow
Raspberry Pi 4 Model B	23:7F:22:CA:EC:3C	yellow
Raspberry Pi 4 Model B	C4:D1:F7:71:9E:5E	yellow
Amazon Echo Dot 4th Gen	BA:21:58:68:5C:41	yellow
Amazon Echo (2020)	2D:6C:BB:AB:AF:0A	yellow

REGISTER YOUR DEVICE

First Name Last Name

Employee ID

Email

Department

Device Floor and Room/Desk

Device Model

Asset Tag Number

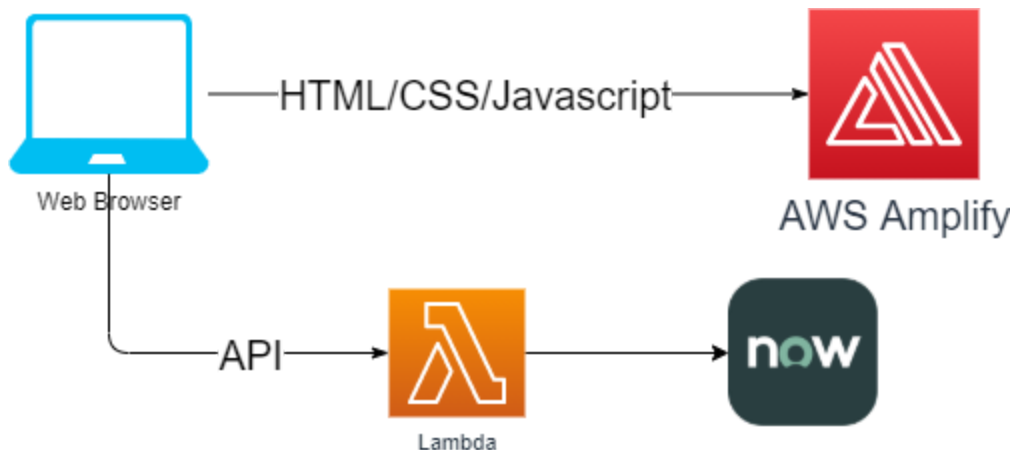
MAC Address

I agree to the [Terms and Conditions](#)

Hosting Solution

Gloco leverages AWS in delivering many of our hosted solutions. The IoT Device management portal will leverage Gloco's existing AWS infrastructure and will use the following platforms:

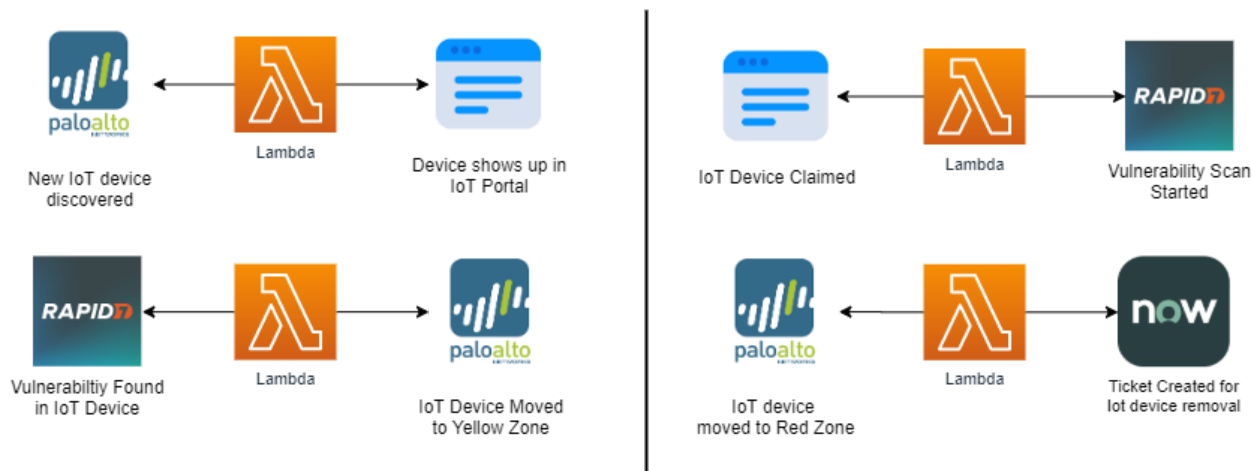
- AWS Amplify will host and serve the website files
- Lambda to provide a Restful API Layer
- ServiceNOW to store IoT device and user assignment information



Summary of Solution

Systems Integrations

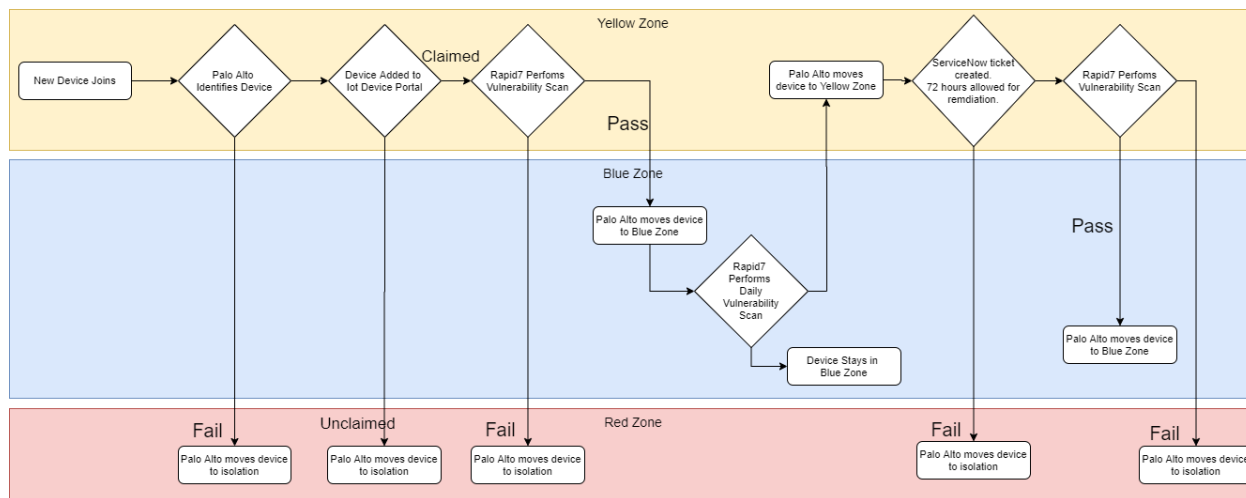
This solution will have multiple platforms that will need to communicate with each other. Every platform has a built in Restful API that can be called. In order to standardize communication between platforms we will be creating AWS Lambdas. Every minute a Lambda will query the given platform asking for new actionable information. The Lambda will take the response and process the information. If there is a required action in a downstream platform, the Lambda will make the appropriate API call to that system. Below are a few examples of some actions a Lambda may make.



Device Workflow Through Zones

1. When a new device joins the network, it is fingerprinted with Palo Alto's Device-ID.
2. The IoT device will be placed in the yellow zone.
 - a. If the device is unable to be identified it will be moved into the red zone.
3. The IoT device will be available for users to claim in the IoT device portal.
4. Once claimed Rapid7 InsightVM will perform a security scan looking for vulnerabilities.
5. If Rapid7 InsightVM finds no vulnerabilities the IoT device is moved into the blue zone.
6. All IoT devices in all the zones will be scanned by Rapid7 InsightVM on a daily basis.
7. If a device is found with vulnerability, it will notify Palo Alto to move the device into the yellow zone for remediation.
8. When a device enters into the yellow zone, a ServiceNow ticket is created for the IT security team and the device owner, alerting them on next steps.

9. If a device is remediated in ServiceNow, Rapid7 InsightVM will re-scan.
10. Based on the scan Rapid7 InsightVM will call Palo Alto to move the device back into the blue zone or send it into the red zone.
11. Devices in the red zone for five days will be physically removed from the network.



PART 3. IMPLEMENTATION PLAN

Solution delivery roadmap

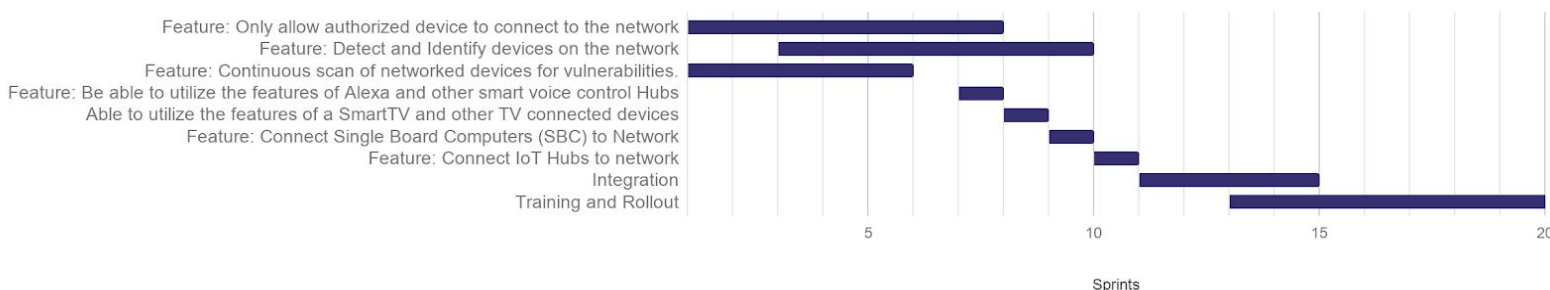
Gloco's I.T. Security team is made up of 26 operational and 10 engineering staff members. SMEs are put in the engineering group and are utilized as an Engineering resource (Tier 4) when needed. Most of the work for this project will be done by the engineering staff with help from the Operations staff. At any given time, during this project, we do not plan on diverting more than 10% of I.T. Security staff to help implement this project.

- For the Palo Alto segment, we will use 1 engineer and 2 operational staff member
- For Rapid7 InsightVM section, we will use 1 engineer and 1 operational staff member
- For Portal creation and setup, we will use 3-4 people from the existing development team.
- For training material creation, we will use 1 person.
- Overall approximately 10 people will be working on the project, expected per week to be between 4-5 people.

Methodology

This project will follow Gloco Scaled Agile Framework (SAFE) development practices. Planning will happen during Gloco's standard product increments (PI) that are 12 weeks long. Sprints will be 2 weeks long and will follow standard Scrum methodology which includes sprint planning, retrospectives and daily standups.

Gantt Chart¹⁰



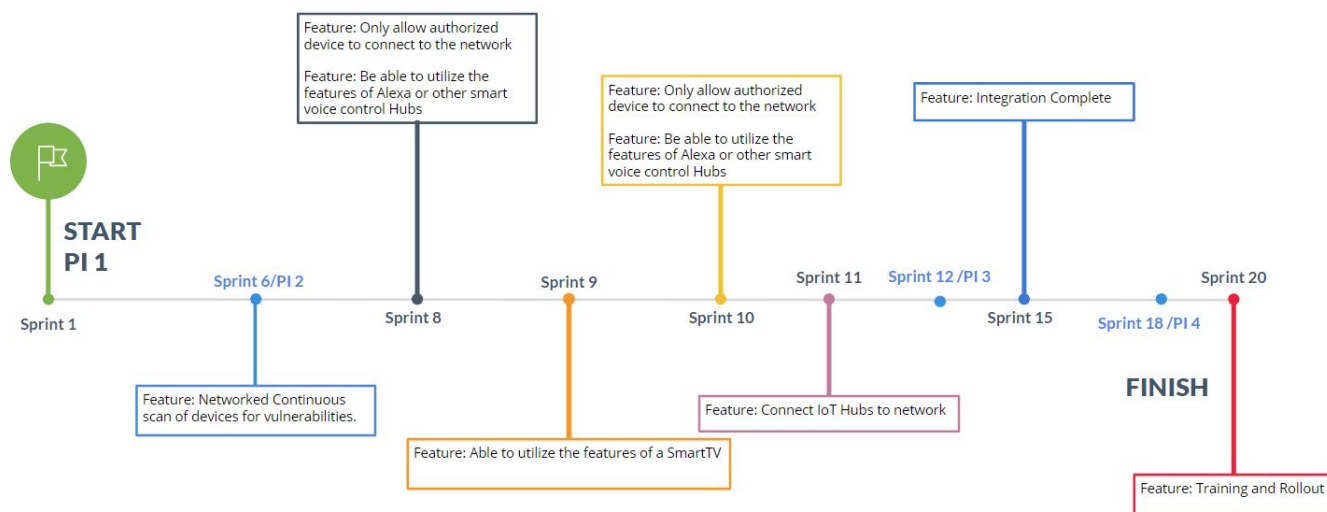
¹⁰ Additional Gantt chart broken down per task can be found in the appendix

Breakdown of Features

TASK NAME	START SPRINT	EST SPRINTS
Feature: Only allow authorized device to connect to the network		
Update to latest Palo Alto OS	1	2
Zone Setup Discovery	3	1
Setup Zones	4	2
Firewall Rules for Blue Zone/Yellow/Red Zone	6	1
Palo Alto Lambda Setup/Connections	7	1
Feature: Detect and Identify devices on the network		
Fingerprinting Setup	3	1
Discovery Scan IoT in Green Zone	4	1
Zone Routing for devices	5	1
Portal Development on AWS	5	1
Portal code and deploy	6	3
Portal Lambda Setup/Connections	9	1
Feature: Continuous scan of networked devices for vulnerabilities.		
Initial Vulnerability Scan	1	1
Setup Zone Vulnerability Scanning	2	2
Schedule and Automate Rapid7 Scans	4	1
Rapid7 Insight Lambda Setup/Connections	5	1
Feature: Be able to utilize the features of Alexa and other smart voice control Hubs		
Configure Firewall for smart voice hubs	7	1
Route voice hubs to correct Zone	7	1
Able to utilize the features of a SmartTV and other TV connected devices		
Configure Firewall for smart voice hubs	8	1
Route SmartTVs to correct Zone	8	1
Feature: Connect Single Board Computers (SBC) to Network		
Configure Firewall for SBC	9	1
RouteSBC to correct Zone	9	1
Feature: Connect IoT Hubs to network		
Configure Firewall for IoT Hubs	10	1
Route IoT Hubs to correct Zone	10	1
Integration		
Full Integration into Gloco Network	11	4
Training and Rollout		
Documentation	13	2
Training Sessions	15	2
Rolling out per office	16	4

Milestones

The majority of the work will be completed over the course of three PIs (18 sprints). Training and documentation will happen during the following PI and will last around two sprints. Below is a breakdown of what sprint features will be completed in.



Inserting the system into company's operational platform

In order to successfully integrate all of the required functionality in Gluco's IoT Security project, we will engage several stakeholders in order to efficiently and effectively provide secure IoT network access for our users. This project has an estimated completion time of 9 months.

- Upgrades will take place during the standard planned maintenance window (Monthly weekend).
- Change Control will involve a meeting with all stakeholders obtaining details with a full plan of action at least 1 month prior to the upgrade. This will provide time for all stakeholders to review the plan and provide any feedback or concerns. Two weeks prior to the scheduled maintenance window, all designated stakeholders can vote on the finalized plan for approval
- As part of our standard outage notifications, Gluco will notify all users of our IoT Security rollout plan via email/Slack/Intranet posts

-
- The implementation plan will get a full test through a lab deployment to ensure our corporate solution including all processes will continue to work
 - Our current configurations will be saved and available on our active and passive firewalls in the event of a failed upgrade or configuration change
 - Our Active/Passive High Availability deployment will eliminate the need for downtime during upgrades. We will implement our zones on a per office basis to reduce inefficiencies created by a large-scale outage
 - Stakeholders will include our project management team, our lead engineers, as well as the department managers of each impacted office during rollout. These department managers will also be responsible for approving IoT devices for their respective organizations

User Enablement: How Will People Use the System

Primarily, this analysis has focused on the technological details that will make the IoT solution possible and the benefits it will provide. It's also important to focus on the final audience: the user base.

The company decided that users can request IoT devices to make the office improve the employee experience. It's up to us as the I.T. Security team to not only keep those devices secure, but also to provide an easy way to add them to the network.

Start Small and Spread

I.T. professionals are aware of how challenging it is to implement new software and processes, but users want it to just work. When new features are rolled out and they work well, the user base is usually quiet, but if any issues arise their collective silence can become an uproar. To protect the user experience, the "IoT@wrk" program will feature a staggered rollout in which it is brought online on an office per office timeline. Also, each office starts with a group of beta users before the full go-live. This approach is slower than others, but it is justified considering that the IoT@wrk program is not an essential business function, it is an employee engagement implementation.

We are leveraging existing platforms that the I.T. Security team has experience working on. The team will receive incremental training from the vendors as part of the rollout/upgrade process.

Throughout Gloco, our departments maintain various company wiki pages on Confluence so our user base is familiar with its functionality. Many of the beta users in the IoT@wrk program volunteered to provide feedback on the process documents and training videos

that will be featured on Confluence. All training materials will be reviewed by the I.T. Security team before publishing.

Keeping Track of the IoTs

All IoT devices are company-owned. To acquire a device, users will visit the ServiceNow request page--the same page used to order a company provided iPad or an ergonomic office chair. If a user brings in an Amazon Echo she got for Christmas, the device will be quarantined in the red zone. Keeping track of company-owned IoT devices will be managed by an asset tag and ownership assigned in ServiceNow. Asset tag stickers are attached to all company-owned laptops, servers, and other devices. The procurement team will attach asset tags to the IoT devices as well.

Alexa has an M.B.A. (Account Management)

AWS offers an Alexa for Business program that "...includes the tools and controls that administrators need to deploy and manage shared Alexa devices, skills, and users at scale."¹¹ Users will create a new Amazon.com account and enroll it with Alexa for Business. Then, they will be invited to join the Gluco Alexa for Business account. For both Amazon and IoT devices from other vendors, the I.T. Security Team will provide an account with a strong password that each user will use. The accounts will be managed by the I.T. security team.

Success Metrics

The main goal for this project is for employees to continue to use IoT devices on premise, while maintaining full visibility in order to prevent any type of attack to Gluco's network. As a result, success metrics are split between security objectives and business value. A company the size of Gluco is a target for malicious attacks. Overlooked high risk devices are an easy entry point for an attacker. To track security success metrics we have created KPIs it needs to hit throughout the fiscal year as well as the annual audit. To measure security benchmarks we will utilize reporting and automation services in Splunk and ServiceNow. This includes creating alerts for specific device events and automating communication to the appropriate people. From an organizational standpoint, employees can securely use these devices on Gluco's network. We measure cost savings of a potential breach as well as the employee experience of using their devices with the new process.

¹¹ <https://aws.amazon.com/alexaforbusiness/faqs/?nc=sn&loc=7>

Security Objectives

Metric	Description	Success Rate
Level of Preparedness	The percentage of devices on the network that are fully patched and up to date.	95%
Mean Time to Detect	How long it takes for a new vulnerability to be detected.	24 hours
Mean Time to Resolve	How long it takes for a user to act once their compromised device is taken off the network	72 hours
Accountability of Devices	This includes all IoT devices on the corporate network and registered devices removed from Gluco premises.	100%
Access Management	Only I.T. Security will have administrative access to the registration portal and registered devices in ServiceNow.	100%
Vendor Patching Cadence	How many risks an IoT device vendor has and how many critical vulnerabilities are yet to be remediated. This is measured by the number of patches found vs the number of patches missing.	95%
Average Risk Score	Rapid7 risk score assigned to each device per daily scan.	Below 7k
Unidentified Devices	Percentage of devices in the yellow zone that have yet to be registered or claimed by an employee.	Below 5%
Internal Audit	Devices found in audit are properly in zones and registered, or removed.	100%

Business Value

Metric	Success Criteria	Success Rate
Cost of Risk	The average cost per breach for a company the size of Gloco is \$3.98 million. Nearly 36% of the average total cost of a security breach comes from lost business. Gloco has over 2 million customer personally identifiable information (PII) records. The average cost per record is \$150 ¹² .	Risk avoidance with savings of almost \$4 million per breach
Reduced LOE	Time it takes for Gloco to identify a new device's owner. Current level of effort without the proposed solution is 20 hours per device. The proposed solution reduces this to almost zero.	Savings of 20 hours of effort per new device
Compliance Savings	Gloco meets all PCI requirements and occurs no PCI compliance fines from an IoT device. ¹³	\$0 in accrued fines
Net Promoter Score	After the rollout we will release a feedback questionnaire regarding the new IoT Security policy and the IoT Device Management Portal. The measurement will be based on employee satisfaction with the new process. The score will be the difference between the percentage of Promoters and Detractors ¹⁴ .	+15 NPS

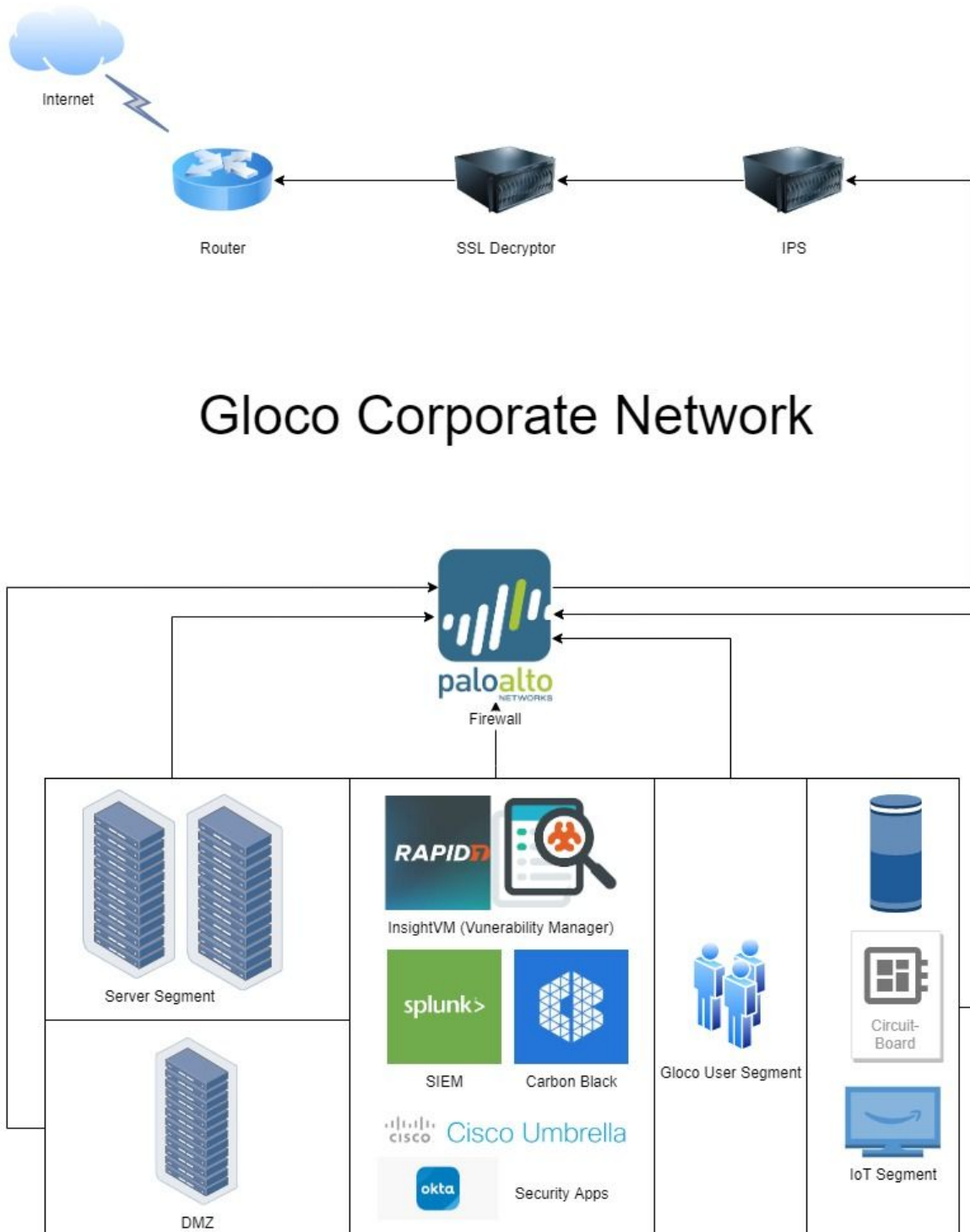
¹² Ponemon Institute. IBM, 2019, *Cost of a Data Breach Report*, www.ibm.com/security/data-breach.

¹³ See PCI Compliance Requirements in Appendix

¹⁴ See Net Promoter Score in Appendix

Appendix

Network Architecture Diagram



Palo Alto Solutions

Vendor Comparison

For the eighth consecutive year Palo Alto Networks is positioned as a leader in the Gartner Magic Quadrant for the Next-Generation Firewall Solution. Their Security Operating Platform is essential to securing Gloco's enterprise network from advanced threats. Their product line extends beyond a standard on-premises solution by providing SD-WAN capabilities to streamline and segment network traffic efficiently. The Zone-based architecture will allow Gloco to segment IoT devices once discovered and then segment them from all other network traffic. The onboard fingerprinting solution is robust enough to identify the rarest of IoT devices, while dynamically applying a security policy based on our Company's risk tolerance. This solution integrates well with other security products and provides additional granularity into our network traffic by correlating Internal Users to their associated IoT devices. The Machine Learning capabilities help the platform create and apply security policies based on a behavior analysis of the identified device.

Functionality	Palo Alto Networks	Check Point Software
Identify IoT Devices	Yes	Yes
Network Segmentation	Yes	Yes
SD-WAN Capability	Yes	Limited
Fingerprinting Capability	Yes	Limited
Identify Users	Yes	Yes
Dynamically Apply Security Policy	Yes	No
Quarantine Vulnerable Devices	Yes	No
Integration into other security products	Yes	Yes
URL Filtering	Yes	Limited
Dedicated Support	Yes	Yes

Vendor Screens

Device Details

The screenshot shows the 'Device Details' page for a Polycom device. The interface includes a sidebar with navigation options like Dashboard, Devices, Profiles, Alerts, Risks, Policy Sets, Applications, Network, Reports, and Administration. The main content area displays the device ID 'Polycom_64167f3d7860' and a risk score of 26. A central image shows a Polycom video conference device. To the right, an 'IDENTITY' section lists details such as Vendor (Polycom Inc.), Model (Trio8800), OS Group (Embedded), MAC Address (04:16:7f:3d:78:60), IP Address (10.72.32.157), Subnet (10.72.32.0/23), and DHCP (Yes). Below this, a 'SECURITY' section shows a risk score of 26, baseline modeling status, and activity dates (First Seen: 03:03 May 20, 2020; Last Activity: 10:58 June 10, 2020). A circular diagram at the bottom left illustrates connections between Software, Applications, Internal Connections, Internet, and Payloads. At the bottom, there are buttons for 'Risks (3)', 'Alerts', and 'Security'.

Device Overview

The screenshot displays the 'Device Overview' page. It features a sidebar with navigation options similar to the previous screen. The main content area is titled 'Devices' and includes filters for 'All Sites', 'All IoT', and '1 Week'. A 'Device Types' section contains a donut chart labeled 'back' and a table showing the distribution of devices. The table has columns for Type, Devices, Categories, Profiles, and Devices at Risk. Below this is an 'Inventory (2,525)' section with a table listing individual devices.

Type	Devices	Categories	Profiles	Devices at Risk	
Office	39 New	1,752	18	30	3
Network Devices	6 New	771	2	8	0

Status	Risk	Device Name	Profile	Vendor	Model	OS	IP Address	MAC Address	VLAN...	Last A...
+	10	NP1358CEE	HP-Printer	Hewlett P...	Laserjet 200 col...	LynxOS	10.55.4.111	d0bf9c358cee	104	Jun 8, 2020
+	10	NP169C180	HP-Printer	Hewlett P...	Laserjet 200 col...	LynxOS	10.55.24.57	a0481c69c180	117	Jun 10, 202
+	38	DESKTOP-2JQEF1N	DTEN Dis...	Intel Corp...	Mocmin7,1	Windows	10.54.100.145	64-5d86fb2267	320	Jun 10, 202

Next Generation Firewall (NGF)

The screenshot shows the PA-220 management interface with the following sections:

- General Information:** Device Name: LAB_RAPPIT, MGT IP Address: 192.168.128.140, MGT Netmask: 255.255.255.0, MGT Default Gateway: 192.168.128.1, MGT IPv6 Address: unknown, MGT IPv6 Link Local Address: fe80:36e5ecfffebe100/64, MGT IPv6 Default Gateway: 34e5ecbe1:00, MGT MAC Address: 34e5ecbe1:00, Model: PA-220, Serial #: [REDACTED], Software Version: 10.0.0, GlobalProtect Agent: 0.0.0, Application Version: 8295-6198 (07/17/20), Threat Version: 8295-6198 (07/17/20), Antivirus Version: 3415-3926 (07/20/20), Device Dictionary Version: 1.211, WildFire Version: 473493-476430 (07/21/20), URL Filtering Version: 20200721.20350, GlobalProtect Clientless VPN Version: 0, Time: Tue Jul 21 19:23:24 2020, Uptime: 0 days, 0:47:31, Device Certificate Status: None.
- System Resources:** Management CPU: 49%.
- Logged In Admins:** Admin: rappahannockit, From: 10.60.0.2, Client: Web, Session Start: 07/21 19:01:39, Idle For: 00:19:57s; rappahannockit, From: 192.168.128.10, Client: Web, Session Start: 07/21 19:23:06, Idle For: 00:00:00s.
- Data Logs:** No data available.
- Threat Logs:** No data available.
- System Logs:**
 - User rappahannockit logged in via Web from 192.168.128.10 using https at 07/21 19:23:06.
 - authenticated for user 'rappahannockit' from 192.168.128.10 at 07/21 19:23:06.
 - PAN-DB was upgraded to version 20200721.20350 at 07/21 19:18:57.
 - PAN-DB was upgraded to version 20200721.20349 at 07/21 19:13:56.
 - Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.128.140 at 19:12:21.
 - PAN-DB was upgraded to version 20200721.20348 at 07/21 19:08:54.
 - NTP sync to server 0.us.pool.ntp.org at 07/21 19:08:31.
 - PAN-DB was upgraded to version 20200721.20346 at 07/21 19:03:52.
 - Connection to Update server: updates.paloaltonetworks.com at 07/21 19:03:52.
- Config Logs:**
 - edit: deviceconfig system device-telemetry at 07/21 19:02:22.
 - override: deviceconfig system device-telemetry at 07/21 19:02:20.
- ACC Risk Factor (Last 60 minutes):** 3.2.
- Top Applications:** Heatmap showing application usage with categories like dns, isp, facebook-base, slack, ms-office, and web.

Rapid7

Vendor Comparison

According to Gartner Rapid7 is a security information and event management leader. They offer multiple products including a vulnerability scanner called InsightVM. It used to be called Nexpose which was an onsite solution but it has been replaced with InsightVM which is hybrid with Cloud and local network presence. What puts InsightVM apart from other vulnerability scanners is their unique threat scoring system which gives each vulnerability a threat score that considers multiple factors e.g. how long the vulnerability has been out, what is the severity of vulnerability, if there is a known exploit and has this exploit been used in the wild? Rapid7 also purchased a very well-known and widely used exploit framework called Metasploit which gives them unique insight into the threat landscape. InsightVM can also integrate with your SCCM infrastructure and help with patching of vulnerabilities and keep track of it all in their dashboards.

Functionality	Rapid 7 - InsightVM	Nessus - Tenable.io
Find vulnerabilities for IoT devices	Yes	Yes
Scoring of threat based on metrics	Yes	No
Accurate Asset discovery and tagging	Yes	No

Risk Management	Yes	No
Cloud based scanner	Yes	Yes
Patch Management Lifecycle	Yes	No
Integration into other security products	Yes	Limited

Rapid7 Screens

Vulnerability Scanning

The screenshot displays the Rapid7 InsightVM interface. At the top, there is a navigation bar with the 'insightVM' logo, a 'Create' dropdown, and various utility icons (search, refresh, home, notifications, help) along with the user name 'Irfan'. Below the navigation bar, there are breadcrumb links: 'Home | View all sites' and 'Full audit without Web Spider | View all scans'.

The main content area is divided into several sections:

- Asset Details:** A grid of information including:
 - ADDRESSES: 192.168.222.189
 - HARDWARE: AC:83:F3:67:77:5A
 - ALIASES
 - SITE: Home
 - UNIQUE IDENTIFIERS
 - SEE ASSET PAGE
 - OS: Ubuntu Linux
 - CPE
 - HOST TYPE: Unknown
 - LAST SCAN: Nov 8, 2020 5:32:56 PM (19 minutes ago)
 - CREDENTIALS
- RISK SCORE:** A section showing 'ORIGINAL' and 'CONTEXT-DRIVEN' risk scores, both set to 11,380.
- USER-ADDED TAGS:** A section with 'CUSTOM TAGS' (Raspberry Pi - IoT), 'LOCATIONS' (Main Office), 'OWNERS' (John Smith), and 'CRITICALITY' (Low). There is an 'Add tags' button.
- VULNERABILITIES:** A table listing various vulnerabilities with columns for 'Vulnerability', 'Severity', and 'Instances'.

Vulnerability	Severity	Instances
Apache HTTPD: ap_get_basic_auth_gw() Authentication Bypass (CVE-2017-3167)	Critical	1
Apache HTTPD: mod_mime Buffer Overread (CVE-2017-7679)	Critical	1
Apache HTTPD: mod_ssl Null Pointer Dereference (CVE-2017-3169)	Critical	1
Apache HTTPD: mod_status buffer overflow (CVE-2014-0226)	Severe	1
Apache HTTPD: Weak Digest auth nonce generation in mod_auth_digest (CVE-2016-1312)	Severe	1
Apache HTTPD: -FilesMatch> bypass with a trailing newline in the file name (CVE-2017-15715)	Severe	1
Apache HTTPD: Uninitialized memory reflection in mod_auth_digest (CVE-2017-9788)	Severe	1
Apache HTTPD: mod_rewrite potential open redirect (CVE-2019-10098)	Severe	1
Apache HTTPD: mod_auth_digest access control bypass (CVE-2019-0217)	Severe	1
Apache HTTPD: mod_rewrite CVE-601 open redirect (CVE-2020-1927)	Severe	1

At the bottom of the interface, there is a pagination control showing 'Showing 1 to 10 of 39' and 'Rows per page: 10'.

Dashboard

50 Assets | 0 Discovered Assets

License Usage: 50 / 73 (66.67%)

1 Sites | 0 Asset Groups | 1 Tagged Assets

ASSET CHARTS

Assessment Status

- Assessed (50)
- Discovered by Scanning (0)
- Discovered by Connection (0)

Assets by Operating System

- Unknown OS (23)
- Google (5)
- Next (4)
- Linux (3)
- Microsoft (3)
- Aruba (2)
- Espressif (2)
- Ubuntu (2)
- Epson (1)
- Other (5)

Exploitable Assets by Skill Level

- Intermediate (1)
- Expert (2)
- No known exploit (46)

SCANNED

Address	Name	Site	Operating System	Vulnerabilities	Risk	Assessed	Last Scan	Delete
192.168.222.189		Home	Ubuntu Linux	0 5 39	11,394	Yes	Sun Nov 8 2020	
192.168.222.108	EPSON7F0E7	Home	Epson 110g/In Print Server	0 1 21	9,738	Yes	Sun Nov 8 2020	
192.168.222.12	FILESERVER	Home	Microsoft Windows Server 2012 R2 Standard Edition	0 1 20	7,692	Yes	Sun Nov 8 2020	
192.168.222.2	SERVER	Home	Microsoft Windows Server 2016 Standard Edition	0 1 13	6,914	Yes	Sun Nov 8 2020	
192.168.222.72	octopi	Home	Respon Linux 10.0	0 0 10	4,387	Yes	Sun Nov 8 2020	
192.168.222.1		Home		0 0 11	3,995	Yes	Sun Nov 8 2020	
192.168.222.114		Home	Linux 3.2	0 0 7	2,957	Yes	Sun Nov 8 2020	
192.168.222.51	Philips Hue	Home	Linux 2.0	0 0 4	1,763	Yes	Sun Nov 8 2020	
192.168.222.83		Home	ArubaOS 6.4.4.8	0 0 4	1,514	Yes	Sun Nov 8 2020	
192.168.222.83		Home	ArubaOS 6.4.4.8	0 0 4	1,514	Yes	Sun Nov 8 2020	

Showing 1 to 10 of 50 | Export to CSV | Rows per page: 10 | 1 of 5

This page contains a breakdown of all vulnerabilities affecting your assets. It is automatically updated with new vulnerabilities as they are discovered. Select a vulnerability to view information about the vulnerabilities and the affected assets.

VULNERABILITY CHARTS

Vulnerabilities by CVSS Score

- 8 - 10 (1)
- 6 - 7.9 (15)
- 4 - 5.9 (28)
- 2 - 3.9 (6)
- 0 - 1.9 (7)

Exploitable Vulnerabilities by Skill Level

- Intermediate (1)
- Expert (4)
- No known exploit (62)

VULNERABILITIES

> Apply Filters (0 applied)

Title	CVSS	CVSSv3	Risk	Published On	Modified On	Severity	Instances	Exceptions
Default or Guessable SNMP community names: public	10	916	Wed Jan 01 1997	Wed Dec 04 2013	Critical	1	Exclude	
SNMP signing disabled	7.3	844	Mon Nov 01 2004	Wed Feb 21 2018	Severe	6	Exclude	
SNMPv2 signing not required	6.2	840	Mon Nov 01 2004	Wed Feb 21 2018	Severe	3	Exclude	
SNMP signing not required	6.2	840	Mon Nov 01 2004	Wed Feb 21 2018	Severe	6	Exclude	
X.509 Certificate Subject CN Does Not Match the Entry Name	7.1	817	Fri Aug 03 2007	Thu Apr 25 2019	Severe	8	Exclude	
Default or Guessable SNMP community names: admin	7.5	758	Wed Jan 01 1997	Wed Dec 04 2013	Critical	1	Exclude	
SNMP credentials transmitted in cleartext	7.5	754	Tue Feb 12 2002	Wed Mar 21 2018	Critical	1	Exclude	
Invalid CPS Logins Permitted	7.5	749	Tue Jan 25 2005	Fri Jul 11 2014	Critical	1	Exclude	
Untrusted TLS/SSL server X.509 certificate	5.8	697	Sun Jan 01 1995	Mon Jul 27 2015	Severe	9	Exclude	
Apache HTTPD: ap_get_basic_auth_jwt() Authentication Bypass (CVE-2017-3167)	7.5	9.8	Tue Jun 20 2017	Mon Jan 08 2018	Critical	1	Exclude	

Showing 1 to 10 of 67 | Export to CSV | Rows per page: 10 | 1 of 7

Okta

User Management

okta Dashboard Directory Applications Devices Security Reports Settings My Applications +

People Help

+ Add Person Reset Passwords Reset Multifactor More Actions

Q Search... All A B C D E F G H I J K L M N O **P** Q R S T U V W X Y Z

FILTERS	Person & Username	Primary Email	Status
Everyone 652	Jessica P. Jones jessica.jones@oktarocks.com	internal user jessica.jones@oktarocks.com	Active
Activated 49	John P. Wick john.wick@oktarocks.com	internal user john.wick@oktarocks.com	Password reset
Pending Activation 0	Nico Powered nico@nicopowered.com	external user nico@nicopowered.com	Active
Password Reset 16			
Deactivated 603			
Suspended 0			
Locked out 0			

Add User

Developer M. Silverman Okta-dev-237330 Documentation & Support Sign out

okta Dashboard Users Applications API Emails & SMS Settings Upgrade

People Help

+ Add Person Reset Passwords

Q Search... Q R S T U V W X Y Z

FILTERS

- Everyone 2
- Activated 2
- Pending Activation 0
- Password Reset -
- Deactivated 0
- Suspended 0
- Locked out 0

Add Person

First name Sally

Last name Admin

Username sally.admin@okta.com

Primary email sally.admin@okta.com

Secondary email (optional) micah@afitnerd.com

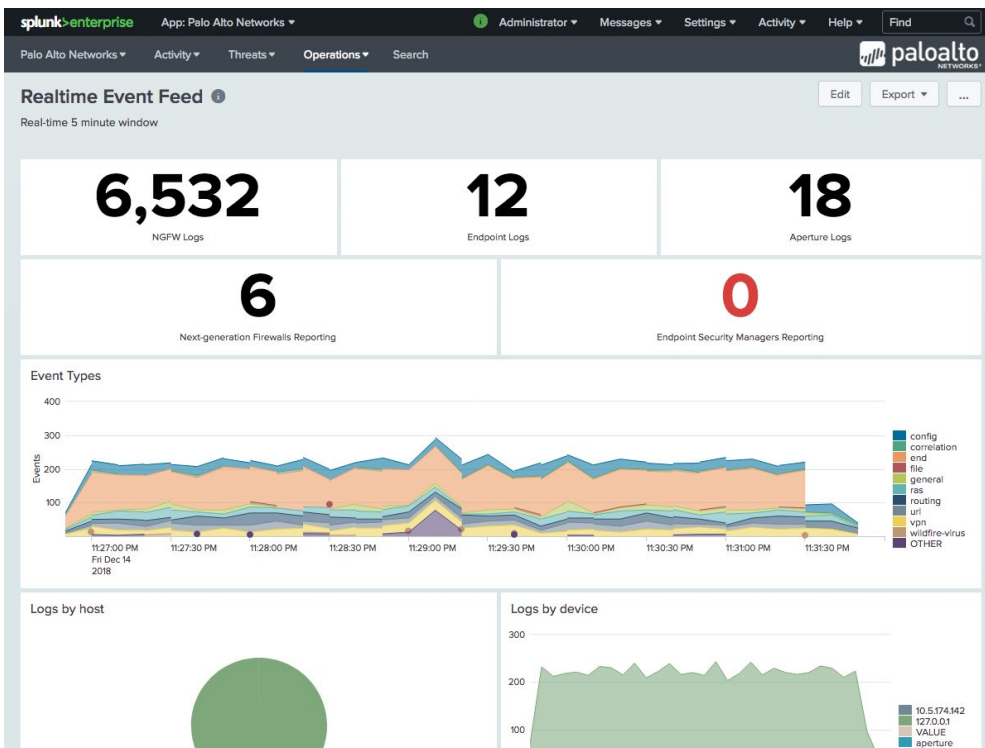
Groups (optional)

users admins

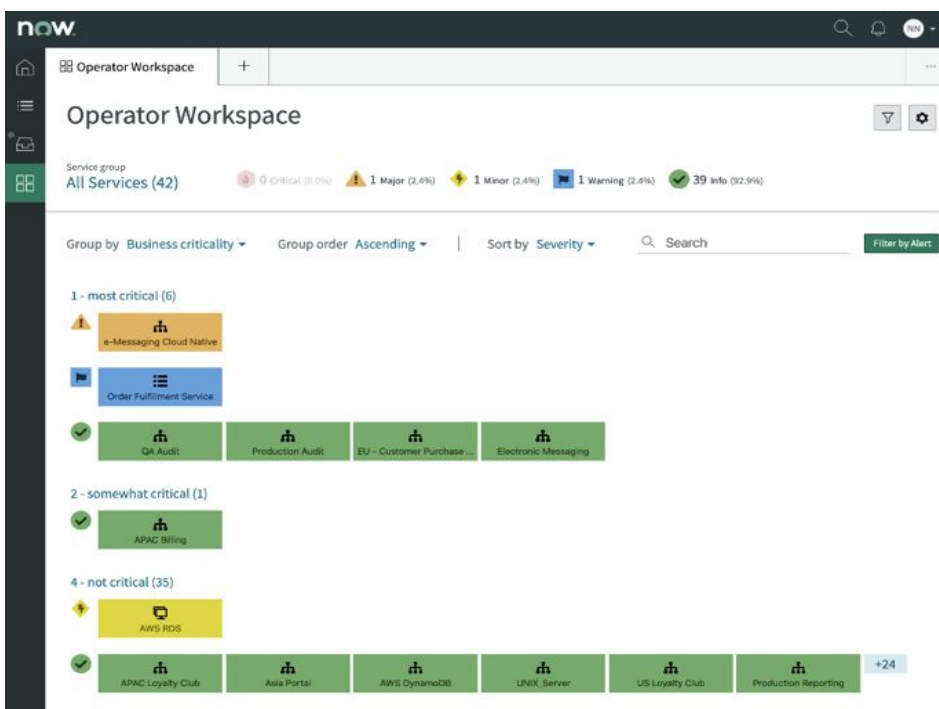
Send user activation email now

Save Save and Add Another Cancel

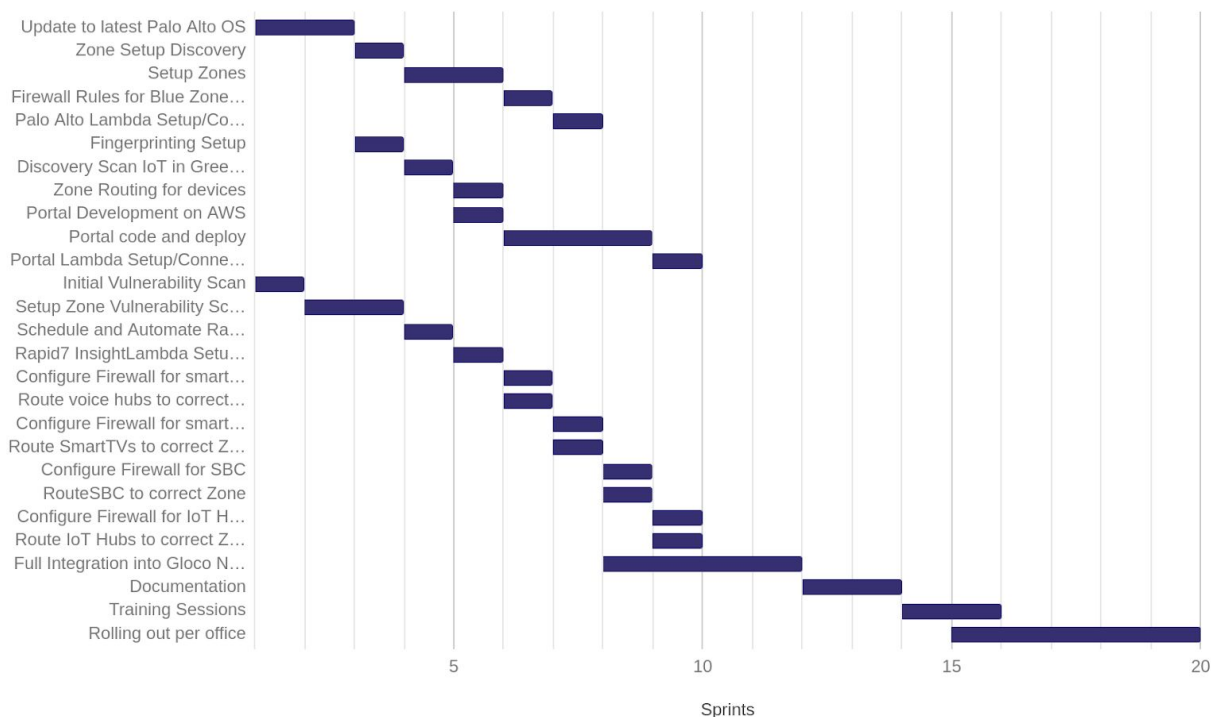
Splunk









ServiceNow



Gantt Chart Per Story



PCI Compliance Requirements

PCI DSS Requirements	
 Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
 Protect cardholder data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
 Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
 Implement strong access control measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.
 Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
 Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel.

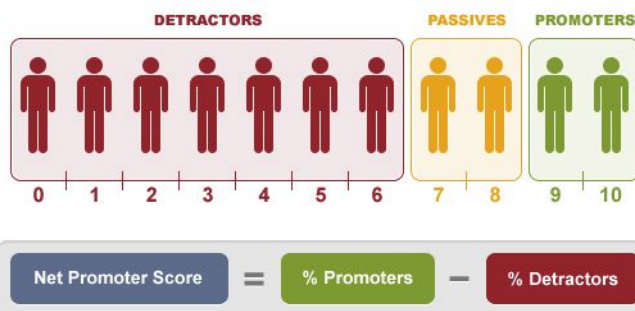
Net Promoter Score

Calculation

Depending on the score that is given to the Net Promoter question, three categories of people can be distinguished:

- Promoters = respondents giving a 9 or 10 score
- Passives = respondents giving a 7 or 8 score
- Detractors = respondents giving a 0 to 6 score

Use our NPS template



The Net Promoter Score is calculated as the difference between the percentage of Promoters and Detractors. The **NPS** is not expressed as a percentage but as an **absolute number** lying between -100 and +100.

For instance, if you have 25% Promoters, 55% Passives and 20% Detractors, the NPS will be +5. A positive NPS (>0) is generally considered as good.