PREVENTION POSTURE ASSESSMENT

Customer XX

xx/xx/xxxx

Table of Contents

Table of Figures

Executive Summary

Key Findings

- 26 out of 82 (31%) technological controls in place provide Full protection for the given stage of the cyberattack lifecycle
- 19 out of 82 (23%) technological controls in place providing Partial protection to some of the enterprise network against stages of the cyberattack lifecycle.
- 37 out of 82 (45%) technological controls have No coverage provided for protection against attacks, according to that component of the cyberattack lifecycle.

Alignment of Findings with the Cyberattack Lifecycle

The below stacked chart provides a high-level overview of the controls listed by group, along with the number of full, partial and no-coverage controls.

Based on the details provided during the interview question-and-answer session, **Customer XX** appears to be weak when protecting against risks and threats from the following areas of the attack lifecycle:

- Privileged Operations and Resource Access
- Exfiltration

While there are control weaknesses found in all areas reviewed, **Customer XX** appears to have better protection in the following areas:

- Delivery (Perimeter Breach)
- Command and Control (Outbound)
- Exploitation and/or Install
- Operations
- Maintenance
- Analytics

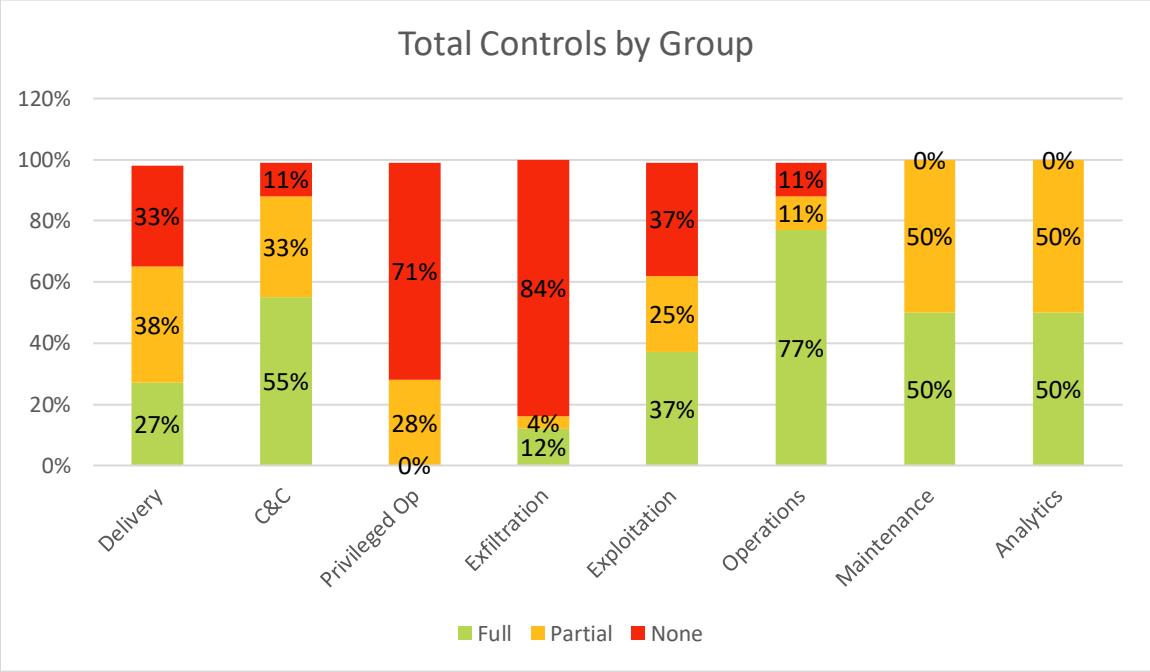

Figure 1: Controls by Grouping

The Prevention Posture Assessment summarizes the business and security risks facing **Customer XX** by documenting key security findings, along with recommendations. Palo Alto Networks® worked with **Customer XX**'s information technology and security staff to gather the data via an interview process.

This report represents a snapshot of the **Customer XX** environment at the time the questions were answered;

The cyberattack lifecycle focuses on a series of techniques, methodologies and processes that attackers follow when attempting to compromise or breach systems.

Customer XX can improve defense against successful attacks by implementing controls that stop attackers at any point in this lifecycle to prevent compromise and data loss via exfiltration. It should be noted that an attacker needs to be successful in all the steps of the attack lifecycle; whereas the defender, needs only to stop them at one step for the attack to be unsuccessful.

This report documents prevention gaps and provides recommendations that teams can implement to improve the security posture and reduce the risk to business operations.

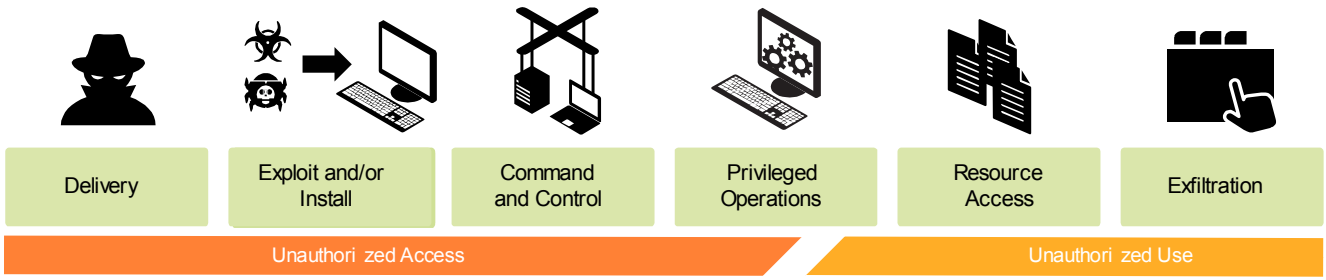

Figure 2: Cyberattack Lifecycle

Enterprise, Mobility and SaaS - Delivery (Perimeter Breach)

This stage focuses on stopping attackers as they attempt to breach the network. Attackers succeed in this stage by reaching out in various ways to users. Many times, this part of the cyberattack lifecycle involves phishing or social-engineering techniques to trick the user into installing malicious files. Our analysis includes the traditional architecture access points, as well as mobile or remote devices, SaaS-based resources, and shadow IT (a term often used to describe information technology systems and solutions built and used inside organizations without explicit organizational approval).

Properly fielding all the capabilities available from Palo Alto Networks Threat Prevention protects across all threat vectors that attackers use to bypass the perimeter of the network – often the first line of defense.

Delivery (Perimeter Breach) Overview Chart

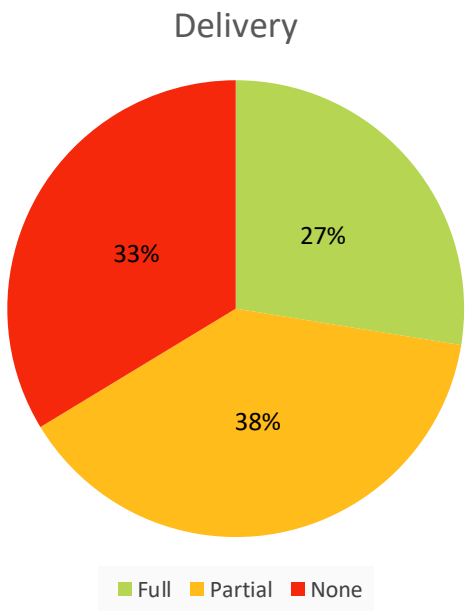

Figure 3: Delivery (Perimeter Breach) Overview Chart

Key Findings

- IPS at all Internet Access Points (1): Vulnerability Protection profiles are configured with critical and high set to blocked and medium, low, informational set to default.
- IPS Extension for Remote Access (2): GlobalProtect is configured in split-tunnel mode so IPS is not enforced on all mobile user traffic. For mobile devices on internal wireless there is IPS done by Checkpoint. It is in the plan to disable split tunnel and channel all the traffic through the firewall via VPN.
- Zero Trust Model Adoption (5): Network segmentation is in place for external and 3rd party networks. Internal network and datacenter are not segmented.
- Perimeter File-Sandboxing (7): WildFire inspection is implemented for all outbound traffic, but bypassed for some flows from servers with direct Internet access. WildFire inspection is implemented for select inbound traffic
- File-Sandboxing Extension for Remote Access (8): GlobalProtect is configured in split-tunnel mode so WildFire inspection is not enforced on all mobile user traffic.

- Decryption (9): All outbound user traffic from the proxies is decrypted. Inbound decryption is implemented for some applications and needs to be expanded further.
- Application Control at Internet Access Points (11): Application control is not fully implemented. The current security policy only blocks known bad applications.
- User Control at Internet Access Points (12): User-ID is currently not enabled due to impact on domain controllers and firewall management plane.
- Identify and Control Unknown Applications at Perimeter (13): There is currently no strategy for handling unknown flows or applications.
- SaaS Application Anti-Malware (15): Netskope is currently being evaluated and will be leveraged for this.
- Email Store/Investigate/Forward (16): Emails are currently being processed by Symantec cloud solution which provides signature-based anti-malware scanning but does not include instant behavioral analysis of unknown files.
- DoS and Reconnaissance Prevention (17): DDOS detection is in place through ISP cloud solution. It is configured in alerting mode only. In addition on-premise DDOS protection functionality is provided by F5 appliances deployed in front of the firewalls.
- Limited Unwanted Network Activity (18): There is no L7 filtering in place for hosted services.

Recommendations

- IPS at all Internet Access Points (1): Review vulnerability protection profiles and verify that critical, high and medium severity events are set to block.
- IPS Extension for Remote Access (2): It is recommended to force all mobile user traffic through the firewall and apply the same controls and policies across all traffic.
    - GlobalProtect Reference Architecture
- Zero Trust Model Adoption (5): Improve the current network segmentation to also include the internal network. A segmentation and zoning workshop can be provided by the Palo Alto Networks Customer Success team.
    - Getting Started With a Zero Trust Approach to Network Security
- Perimeter File-Sandboxing (7): Continue implementation of WildFire file forwarding on any remaining flows.
- File-Sandboxing Extension for Remote Access (8): It is recommended to force all mobile user traffic through the firewall and apply the same controls and policies across all traffic.
- Decryption (9): Identify additional inbound SSL flows and enable decryption for those flows.
    - Configure SSL Inbound Inspection
- Application Control at Internet Access Points (11): Improve current application control strategy and move to a possitive application enforcement approach, starting with most critical zones.
- User Control at Internet Access Points (12): Implement User-ID and improve current security policy by controlling network access based on user groups.
- Identify and Control Unknown Applications at Perimeter (13): Implement a process to alert on and review outbound unknown tcp and udp sessions.
    - Unknown Applications
- Email Store/Investigate/Forward (16): Inpsect SMTP flows with WildFire and enable forwarding for both attachments and email-links.
- DoS and Reconnaissance Prevention (17): Implement Zone and DoS Protection to reduce the impact of reconnaissance probes, floods and packet based attacks on the firewall.
    - Understanding DoS Protection
    - Zone Protection Documentation
    - Best practices for securing your network from layer-4 and layer-7 evasions.
- Limited Unwanted Network Activity (18): Implement L7 filtering capabilities such as App-ID and Threat Prevention to improve protection for hosted services.

Section	Capability	Q.No	Current State	Future State
Delivery (Perimeter Breach)	IPS (All ports, inline, both sides of traffic)	1	Partial	Full
		2	Partial	Full
		3	Full	Full
	URL Filtering (All ports)	4	Full	Full
	Segmentation (Zones)	5	Partial	Full
	Anti-Malware (All ports and inline)	6	Full	Full
	Sandboxing (All ports and inline)	7	Partial	Full
		8	None	Full
	Decryption	9	Partial	Full
		10	Full	Full
	User and Application Control (Layer 7)	11	None	Partial
		12	None	Partial
		13	None	Partial
		14	Full	Full
	SaaS malware delivery protection	15	None	Full
	E-mail store and forward	16	Partial	Full
	Infrastructure Protection (Zones)	17	Partial	Full
	Hosted Service Protection (Internal Zones)	18	None	Full

Figure 4: Delivery (Perimeter Breach) Stage Gaps

Enterprise, Mobility and SaaS - Command and Control (Outbound)

This stage focuses on stopping an attacker from communicating with a compromised computer through a command and control channel. Most modern day malware now leverages SSL (Secure Socket Layer) to communicate over a secure encrypted tunnel keeping many security solutions blind to attacker activity. Some malware command and control also tries to impersonate other well-known protocols that are often not monitored by security solutions

focused on a limited number of ports. A perfect example of this is the high number of command and control traffic today that takes advantage of organizations opening DNS to the Internet. DNS (port 53) is one of the most widely used ports by malware, as a large number of companies never monitor this for security risks.

Palo Alto Networks solutions allow you to easily control which protocol can use which port and protect across all ports, regardless of protocol.

Command and Control (Outbound) Overview Chart

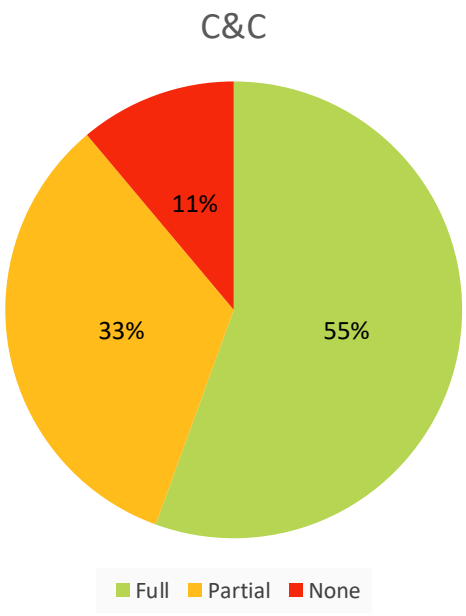

Figure 5: Command and Control (Outbound) Overview Chart

Key Findings

- IPS Inspection for Command and Control Activity (19): DNS sinkholing is configured but requires review. All Anti-spyware profiles require a review.
- Investigate Unknown URL for Malicious Behaviors (20): Unknown URLs are alerted on, but no block is applied or continue page presented. Investigation is done manually by correlating firewall and proxy logs through the SIEM.
- Logging Only URL Container Page (22): Only container pages are logged on the firewalls. The entire URL is logged on the proxies.
- Dynamically Update IP, Domain, and URL Block Lists (24): A process is in place to update URL block lists on the proxies. Nothing currently on the firewall, but Minemeld options are being investigated.
- Remediate Unknown TCP/UDP (25): There is currently no process in place to investigate and eliminate unknown tcp and udp sessions.
- Prevention of Post-Compromise Malware Delivery (26): SSL decryption policy is in place for outbound traffic, but can be improved and expanded.

Recommendations

- IPS Inspection for Command and Control Activity (19): Review Anti-Spyware profiles and verify Critical, High and Medium severity events are blocked. Verify that Anti-Spyware is enabled for all traffic.
- Investigate Unknown URL for Malicious Behaviors (20): Configure WildFire forwarding of email-links to detect malicious URLS at an earlier stage in the cyberattack lifecycle. This requires WildFire to be enabled for inbound SMTP traffic.

- Dynamically Update IP, Domain, and URL Block Lists (24): Investigate options to automate inclusion of 3rd party feeds with customer managed blocklists. Complement existing URL lists with IP and domain lists on the firewall.
    - Minemeld Product Page
    - Autofocus-Hosted Minemeld
- Remediate Unknown TCP/UDP (25): Implement a process to alert on and review outbound unknown tcp and udp sessions.
    - Unknown Applications
- Prevention of Post-Compromise Malware Delivery (26): Continue expansion of SSL decryption and the use of decryption profiles to decrypt and prevent delivery of malware over SSL.
- Prevention of Post-Compromise Malware Delivery (26): Review the security policy to ensure that allowed proxy bypass flows are fully decrypted and inspected.

Section	Capability	Q.No	Current State	Future State
Command and Control (Outbound)	IPS (All ports and inline)	19	Partial	Full
	URL Filtering (All ports)	20	Full	Full
		21	Full	Full
		22	Full	Full
		23	Full	Full
		24	Partial	Full
	Unknown App Blocking	25	None	Partial
		26	Partial	Full
	Unauthorized App Blocking	27	Full	Full

Figure 6: Command and Control (Outbound) Stage Gaps

Enterprise, Mobility and SaaS - Privileged Operations and Resource Access

This stage focuses on preventing an attacker from moving from one point to another inside a network. The attacker intention at this stage is to move laterally (east-west) until they reach their ultimate goal of data center access. A key component of this stage is the ability to segment users and applications as well as any traffic coming in or out of the data center. Protecting the internal assets through segmentation needs to occur whether the data center workload exists on premises, hosted or in the cloud.

Privileged Operations and Resource Access Overview Chart

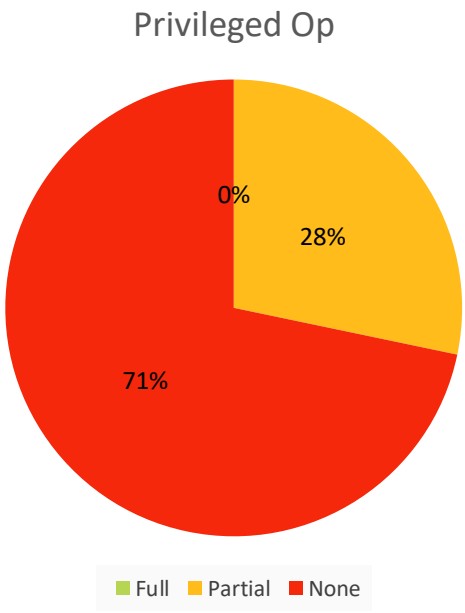

Figure 7: Privileged Operations and Resource Access Overview Chart

Key Findings

- Lateral Traffic Security Enforcement and IPS (28): Firewall segmentation and IPS are in place for external and 3rd party networks, but there is currently no segmentation of internal traffic. Vulnerability protection profiles require a review for all segmentation firewalls currently in place.
- Internal Anti-Malware Protection (29): Firewall segmentation and AV are in place for external and 3rd party networks, but there is currently no segmentation of internal traffic. Antivirus profiles require a review for all segmentation firewalls currently in place.
- Internal File-Sandboxing (30): There is currently no segmentation of internal traffic. WildFire is only implemented on external firewalls.
- Credential Theft Protection (31): Internal applications are not enabled to use Multi-factor Authentication, nor is this capability deployed on a network level.
- Internal Granular Control of Applications and Functions (33): The intention is there to enable application control but there are some App-ID related challenges to overcome.
- Internal Control of User based on Business Needs (34): User-ID is currently not enabled due to impact on domain controllers and firewall management plane.

Recommendations

- Lateral Traffic Security Enforcement and IPS (28): Improve the current network segmentation to also include the internal network.
- Lateral Traffic Security Enforcement and IPS (28): Review Vulnerability Protection profiles and verify Critical, High and Medium severity events are blocked. Verify that Vulnerability Protection is enabled for all traffic.
- Internal Anti-Malware Protection (29): Review Vulnerability Protection profiles and both AV and WildFire events are blocked. Verify that Antivirus is enabled for all traffic.
- Internal File-Sandboxing (30): Develop and implement a strategy to perform sandboxing of files extracted from internal network traffic.

- Credential Theft Protection (31): Review new functionality in PAN-OS 8.0 and investigate feasibility to implement credential theft and abuse protection capabilities. This includes analyzing email-links with WildFire, blocking phishing URLs, blocking credential theft and preventing credential abuse through Multi-Factor authentication.
    - Preventing Credential-Based Attacks
- Internal User and Application based Segmentation (32): Improve the current network segmentation to also include the internal network.
- Internal User and Application based Segmentation (32): Develop and implement a strategy to segment the internal core by user and application.
- Internal Granular Control of Applications and Functions (33): Develop and implement a strategy for controlling applications on the internal network.
- Internal Control of User based on Business Needs (34): Develop and implement a strategy for controlling user access to the network.

Section	Capability	Q.No	Current State	Future State
Privileged Operations and Resource Access	IPS (All ports and inline)	28	Partial	Full
	Anti-Malware (All ports and inline)	29	Partial	Full
	Sandboxing (All ports and inline)	30	None	Full
	Credential Theft Protection	31	None	Partial
	Segmentation	32	None	Partial
	User and Application Control (Layer 7)	33	None	Partial
		34	None	Partial

Figure 8: Privileged Operations and Resource Access Stage Gaps

Data Center, Cloud and SaaS - Exfiltration

This stage focuses on preventing an attacker from removing the business-critical data from the business. Protecting business-critical information in the Data Center is critical. History has shown that failure at this stage of the cyberattack lifecycle was the costliest. This kind of failure has the potential to negatively affect the company's stock price for the business through legal requirements.

Exfiltration Overview Chart

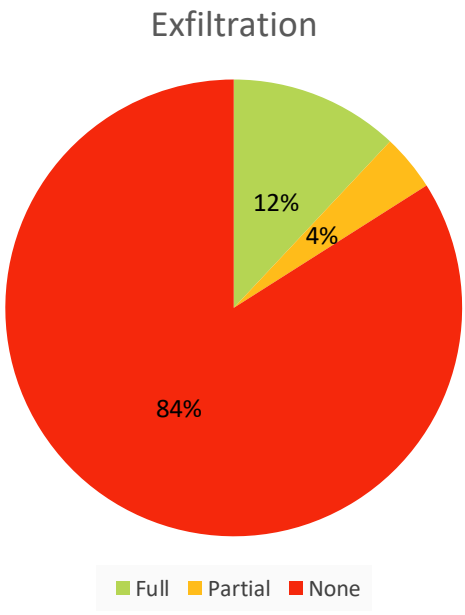

Figure 9: Exfiltration Overview Chart

Key Findings

- DC North/South IPS (35): Firewall segmentation and IPS are in place for external and 3rd party networks, but there is no segmentation between the internal network and the datacenter.
- DC Application Control Policy (36): Limited set of rules is in place for external and 3rd party networks, but not for internal users.
- DC User Control Policy (37): Some restrictions are set at applications level based on Active Directory groups, but no user access control at the network level.
- Micro-Segmentation of DC (38): No host isolation is done in the datacenter.
- DC East/West IPS (39): There is no IPS and segmentation between servers or application tiers in the datacenter.
- DC East/West and North/South Anti-Malware (40): There is no anti-malware and segmentation between servers or application tiers in the datacenter.
- DC East/West and North/South File-Sandboxing (41): There is no sandboxing and segmentation between servers or application tiers in the datacenter.
- Security Extension for Surge Operations (43): An initiative to explore available cloud solutions is ongoing.
- Organization Drivers for Cloud Adoption (46): More details needed.
- General Securing of Public Cloud (47): More details needed.
- Visibility into Public Cloud Applications (48): More details needed.
- Segmentation or Whitelisting of Public Cloud (49): More details needed.
- IPS/AV/Anti-Malware for Public Cloud (50): More details needed.
- File-Sandboxing for Public Cloud (51): More details needed.
- Automation of Standard Security Policies in Public Cloud (52): More details needed.
- Sanctioned SaaS Application List (53): A list of sanctioned SaaS applications is available, but no governance or control is in place to limit unsanctioned applications. Netskope is currently being evaluated and will be leveraged for this.

- Sanctioned SaaS User Activity Visibility (54): No visibility into user activity for sanctioned SaaS applications. Netskope is currently being evaluated and will be leveraged for this.
- Sanctioned SaaS Sensitive Content Control (55): No data protection policies have been defined yet for SaaS applications. Netskope is currently being evaluated and will be leveraged for this.
- Sanctioned SaaS Content Sharing Control (56): No data protection policies have been defined yet for SaaS applications. Netskope is currently being evaluated and will be leveraged for this.
- Sanctioned SaaS Sensitive Content Public Share Control (57): No data protection policies have been defined yet for SaaS applications. Netskope is currently being evaluated and will be leveraged for this.
- Unsanctioned SaaS Application Control (58): No visibility into unsanctioned SaaS application traffic. Netskope is currently being evaluated and will be leveraged for this.
- SaaS Governance and Policies (59): No enforcement of SaaS governance and policies currently. Netskope is currently being evaluated and will be leveraged for this.

Recommendations

- DC North/South IPS (35): Develop and implement an internal network and datacenter segmentation strategy.
- DC North/South IPS (35): Implement Vulnerability Protection for all north-south traffic in the datacenter.
- DC Application Control Policy (36): Develop and implement an internal network and datacenter segmentation strategy.
- DC Application Control Policy (36): Develop and implement an application control strategy for applications hosted in the DC.
- DC User Control Policy (37): Develop and implement an user access strategy for applications hosted in the DC.
- DC East/West IPS (39): Develop and implement a segmentation strategy for intra DC communication.
- DC East/West IPS (39): Implement Vulnerability Protection for all east-west traffic in the datacenter.
- DC East/West and North/South Anti-Malware (40): Implement Antivirus for all east-west traffic in the datacenter.
- DC East/West and North/South File-Sandboxing (41): Develop and implement a strategy to perform sandboxing of files extracted from intra DC network traffic.
- Security Extension for Surge Operations (43): Investigate options for automated security provisioning.

Section	Capability	Q.No	Current State	Future State
Exfiltration	North/South IPS (All ports and inline)	35	None	Partial
	User and Application Control (Layer 7)	36	None	Partial
		37	None	Partial
	Micro-segmentation	38	None	None
	East/West IPS (All ports and inline)	39	None	Partial
	Anti-Malware (All ports and inline)	40	None	Partial
	Sandboxing (All ports and inline)	41	None	Partial
	Automated Demand	42	Full	Full

	Provisioning			
	Automated Extension of Policy, Security and Micro-segmentation for Surge Operations	43	None	Partial
	Public Cloud Strategy (AWS, Azure)	44	Full	Full
		45	Full	Full
		46	None	None
	Public Cloud Protection, Visibility, and Control	47	None	None
		48	None	None
		49	None	None
		50	None	None
		51	None	None
		52	None	None
	SaaS IT Sanctioned (Box, Dropbox, Google Drive, GitHub, Salesforce, Yammer)	53	Partial	Full
		54	None	Full
		55	None	Full
		56	None	Full
		57	None	Full
	SaaS IT Unsanctioned (Zippyshare, 4share)	58	None	Full
	SaaS Enforcement and Reporting	59	None	Full

Figure 10: Exfiltration Stage Gaps

Endpoint(Workstations/Servers) - Exploitation and/or Install

This stage of the attack lifecycle focuses on what can be allowed on the endpoint to prevent breaches. It requires that the company not be reliant upon traditional AV-based, signature-scanning technologies, which are reliable stop-gap solutions about 24–50 percent of the time when a virus is first seen. **Customer XX** instead should focus on an endpoint solution that stops exploit techniques – the tools today's attackers use to compromise hosts through common, yet advanced, methods.

Stopping malware based on traditional product offerings often requires a one-to-one signature relationship. As malware continues to morph, thought-programming changes or in-the-wild, traditional antivirus technologies need to release new signatures for existing malware. Palo Alto Networks Traps™ advanced endpoint protection is focused on exploit preventions (the same techniques that malware writers use), so that preventing only one of the many techniques needed to compromise a system prevents the malware from being successful. This exploit focus also limits the number of signatures needed to block a larger number of malicious files.

Exploitation and/or Install Overview Chart

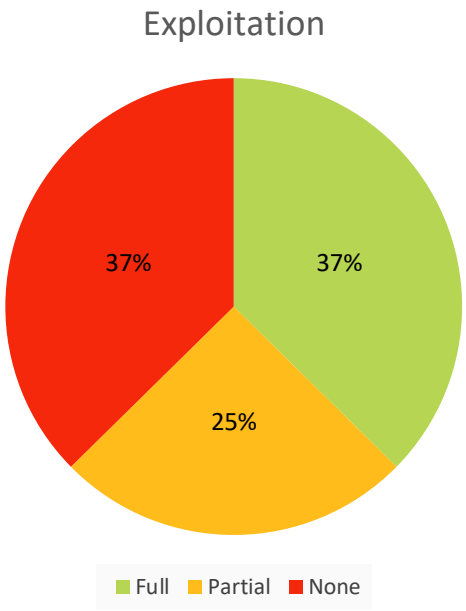

Figure 11: Exploitation and/or Install Overview Chart

Key Findings

- Exploit Prevention on Physical Hosts (60): No exploit prevention capability is implemented on workstations. TRAPS is deployed on the servers.
- Exploit Prevention on Virtual Hosts (61): TRAPS is deployed on the virtualized servers. There is no exploit prevention deployed on the VDI servers.
- Endpoint File-Sandboxing (63): Unknown executables are not being investigated prior to execution.
- Endpoint Malicious Indicators Distribution (64): There is no endpoint solution in place that can be updated in near real-time based on ad-hoc analysis of unknown malware.
- Endpoint Application and Whitelisting Control (65): No validation of executables is performed against whitelists prior to execution.

Recommendations

- Exploit Prevention on Physical Hosts (60): Develop and implement an exploit prevention strategy for workstations.
    - TRAPS Technology Overview
- Exploit Prevention on Virtual Hosts (61): Deploy exploit prevention capability on VDI servers as well.
- Endpoint File-Sandboxing (63): Develop and implement a strategy for handling unknown executables on endpoints.
- Endpoint Malicious Indicators Distribution (64): Implement an endpoint solution that can leverage instant indicator updates found during analysis of unknown malicious executables.

- Endpoint Application and Whitelisting Control (65): Implement an endpoint solution that can validate executables against known good whitelists prior to execution.

Section	Capability	Q.No	Current State	Future State
Exploitation and/or Install	Exploit Prevention (Physical Workstations and Servers)	60	Partial	Full
	Exploit Prevention (Virtual Workstations and Servers)	61	Partial	Full
	Outdated Windows Servers and Workstations	62	Full	Full
	Sandboxing	63	None	Partial
	Sandbox Indicator Scaling	64	None	Partial
	Endpoint Application Control	65	None	Partial
	Endpoint Control and Restrictions	66	Full	Full
	Anti-Malware	67	Full	Full

Figure 12: Exploitation and/or Install Stage Gaps

Operational Fundamentals - Operations

Operations Overview Chart

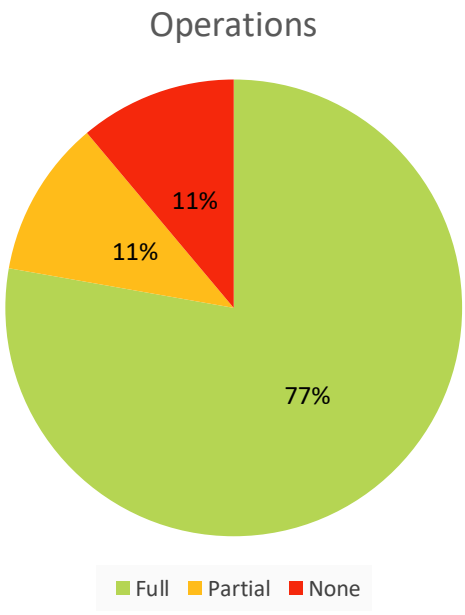

Figure 13: Operations Overview Chart

Key Findings

- Login Banner (70): Panorama config review shows there is no login banner configured for 3rdpartygateway, CTI-Core-Internet and CTI-Regional-FWs templates.
- Rule Tagging Practice (74): Some tagging is in place, but intention is to develop and implement a global tagging strategy.
- Panorama Connect Devices Health Check (76): Alerts are currently send via 3rd party tool that checks connectivity to Panorama.

Recommendations

- Login Banner (70): Configure login banners in Panorama for all device templates.
- Local Admin Account Backup (73): Implementing a second local account could be considered for redundancy.
- Rule Tagging Practice (74): Develop and implement a rule tagging strategy. The Customer Success team can organize a tagging workshop and provide input to creating a rule tagging strategy.
- Panorama Connect Devices Health Check (76): Consider forwarding medium, high and critical system log events from the firewalls via syslog or snmp and alert on Panorama connectivity failures.
- Panorama Connect Devices Health Check (76): Consider forwarding medium, high and critical system log events from Panorama to monitoring solution via syslog or SNMP and alert on health-related events.

Section	Capability	Q.No	Current State	Future State
Operations	Management Access	68	Full	Full
		69	Full	Full
		70	Partial	Full

	Admin Authentication	71	Full	Full
		72	Full	Full
		73	Full	Full
	Organization	74	None	Partial
	Status Check	75	Full	Full
	Panorama	76	Full	Full

Figure 14: Operations Stage Gaps

Operational Fundamentals - Maintenance

Maintenance Overview Chart

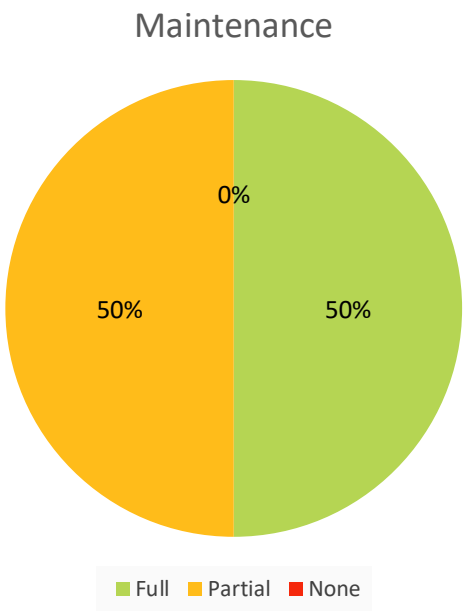

Figure 15: Maintenance Overview Chart

Key Findings

- Dynamic Updates Schedule (78): AV every day; WF every 15 mins; TP 1 week Panorama config review shows that not all firewalls have dynamic update schedules configured and no central deployment schedules are configured on Panorama.
- External Log Backup (80): Panorama config review shows not all firewalls and Panorama are configured to forward system and config logs to SIEM tool.

Recommendations

- Dynamic Updates Schedule (78): It is recommended to check for TP updates every day, AV updates every hour and WildFire updates every minute.
- Dynamic Updates Schedule (78): Review Dynamic Update schedules for all firewalls and ensure recommended update schedules are configured either via device template or via Panorama central deployment schedules.
- External Log Backup (80): It is recommended to forward all firewall and Panorama system and config logs to a SIEM tool.

Section	Capability	Q.No	Current State	Future State
Maintenance	Backup	77	Full	Full
	Content Update	78	Partial	Full
	Software Update	79	Full	Full
	Log Export	80	Partial	Full

Figure 16: Maintenance Stage Gaps

Operational Fundamentals - Analytics

Analytics Overview Chart

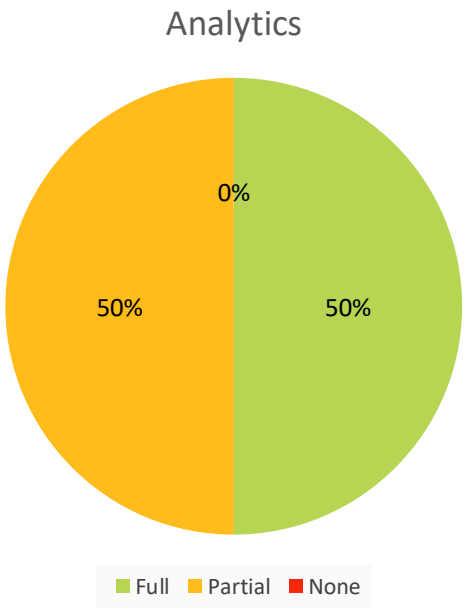

Figure 17: Analytics Overview Chart

Key Findings

- Global Log Correlation and Intelligence (82): Autofocus license is in place but WF is not deployed everywhere yet.

Recommendations

- Global Log Correlation and Intelligence (82): Leverage Autofocus as a threat intel and analytics tool and integrate it into the current incident analysis and response workflow.
- Global Log Correlation and Intelligence (82): Minemeld can be leveraged to automate the aggregation and distribution of Autofocus IOCs with 3rd party feeds and IOCs created by internal SOC.

Section	Capability	Q.No	Current State	Future State
Analytics	Analytics and Correlation	81	Full	Full
	Analytics and Global Intelligence Sharing	82	Partial	Full

Figure 18: Analytics Stage Gaps