Current Cyber Security Risks

1. NAC (Network Access Control)

- **Barracuda** free MDM and/or next-gen firewall with SSLVPN NAC
- **FortiNet** FortiClient is the endpoint client and enforces NAC based on set rules
- **Palo Alto** TRAPS offers exploit and malware endpoint protection. GlobalProtect offers NAC from the firewall.
- **Panda Security** No dedicated NAC solution but does detailed monitoring of sockets opened by applications (includes GeoLocation) that the customer can used with 3rd party monitoring solutions.
- **Sophos** SG or XG next-gen unified threat management firewall

2. Encryption

- **Barracuda** Email Security Service and Email Security Gateway offer decryption of emails.
- **BitDefender** Bitdefender's GravityZone endpoint protection platform will be adding full-disk encryption capabilities for Windows and Mac in June, 2017. It will be a policy engine for enforcing the native Bitlocker (Windows) and FileVault (Mac) encryption systems.
- **FortiNet** FortiGate supports multiple levels of encryption and FortiMail supports Identity Based Encryption (IBE) to encrypt emails
- **Palo Alto** can decrypt on the firewall side with a public CA.
- **Sophos** Safeguard encryption (cloud and on-prem offerings)

3. Lateral Movement of Data

- **Barracuda** Next-gen firewall can prevent cyber intrusion. Network segmentation, defined user based roles, prevent vulnerability scanning and block peer to peer malware.
- **BitDefender**
- **FortiNet** FortiGate can be used for internal segmentation and handles 1terabit per second stateful inspection
- **Palo Alto** has VM based firewalls to protect laterally. Traps will catch malicious files with the AntiMalware component which leverages WildFire which has machine learning capabilities.
- **Panda Security** covered with Adaptive Defense,
- **Sophos** Safeguard to encrypt data

4. Recursive DNS

- **Barracuda** Next-gen firewall offers a DNS service
- **FortiNet** FortiGate support recursive DNS but doesn't have a DNS service
- **Palo Alto** perform this with AntiSpyware on the firewall. Endpoints behind the firewall and on GlobalProtect would be scanned. This effectively allows to protect against command and control channels to be established.
- **Panda Security** NextGen Adaptive Defense provides DNS reputation and file types opened

5. AntiVirus / Endpoint Protection

- **Barracuda** Subscription based and automatically updates with latest signatures. Perimeter protection only (doesn't protect the end user device, only the network perimeter)
- **BitDefender** Bitdefender's GravityZone endpoint protection platform provides an extremely thorough and layered approach to malware detection and is well known for its detection rate, low resource utilization, and ease of management. It runs on Windows, Linux, and Mac and is particularly well suited for virtualized datacenter environments.
- **FortiNet** FortiLabs is a dedicated team of 300 engineers that maintain a current signature base of signatures. FortiNet doesn't outsource any of their intelligence. FortiSandBox comes in on-prem and cloud based versions and protects against zero day threats
- **Palo Alto***
- **Panda Security** Full anti-malware suite within Endpoint Protection Plus offer plus included in the Adaptive Defense 360 product, combining EDR with NextGen AntiVirus.
- **Sophos** Central AV +Ransomware Protection (cloud or on-prem)

5. AntiVirus / Endpoint Protection (cont'd)

- **Palo Alto** TRAPS client protects the end user devices, can be upgraded with the WildFire subscription to use WildFire Threat Intelligence hash checking on known threats and WildFire Sandbox for unknown threats to help with finding any zero day malicious code
  - Traps performs both exploit & malware prevention using the following technologies:
    - Malware Protection Policy
    - Restriction Policy checking
    - Local Analysis using Machine Learning
    - Signed Vendors
    - Admin Overrides
    - Security Features
    - Microsoft Office File Protection
    - Enhanced Child Process Protection
    - Exploit Kit Fingerprinting Protection
    - Kernel Privilege Escalation Protection
    - Dylib-Hijacking Protection
    - Gatekeeper Enhancement
    - Traps Registration with Microsoft Security Center

Current Cyber Security Risks

6. Whitelisting

- **Barracuda** Use with extreme caution, creates a hole in the firewall
- **BitDefender** Bitdefender's GravityZone platform provides a number of endpoint protection features, including Application Whitelisting. Applications are tracked by hash, so it cannot be circumvented by changing names. Authorized Updaters can be assigned, so that when they update an application, those are automatically added to the whitelist.
- **FortiNet** FortiGate uses FortiGuard category filtering and will accept blacklist and whitelists. FortiClient enforces these rules, even when the client is off network.
- **Palo Alto** Traps offers restriction policies which can allow admins to block executables from running in certain locations such as user desktop or temp directory
- **Panda Security** Adaptive Defense, delivered in an innovative way as "Managed Whitelisting". Adaptive Defense will classify 100% of all running applications and potentially allow execution only of executables classified as goodware – that is, that have a goodware reputation in our cloud and/or which behavior lies within the pattern we are monitoring worldwide from our Big Data environment for all the endpoints covered by the service
- **Sophos** SG / XG next-gen firewall has whitelist capability and endpoint whitelisting for clients.

8. SIEM (Security Information and Event Management)

- **Barracuda** Next-gen firewall control center syslog or export logs to a dedicated syslog server (Barracuda integrates with many)
- **BitDefender** Bitdefender's GravityZone endpoint protection platform is not a SIEM, but we do integrate with SIEMs by senidng our notifications to syslog servers. We also have extensive reporting and notifications for the areas which we do cover, which include antimalware, web content filtering, host based firewall, device control, Exchange protection, and iOS / Android mobile device management.
- **FortiNet** FortiSIEM handles reporting and event management and can be scheduled to send reports to the appropriate person.
- **Palo Alto** partner with Splunk who offers an app that ESM can send events to as well as Panorama which can take events from ESM and firewalls then send them off box to Splunk
- **Panda Security** Adaptive Defense context, both delivering a dedicated SIEM environment for its data with our Advanced Reporting Tool or with the ability to integrate the monitoring data generated by Adaptive Defense with 3rd party solutions through our SIEMFeeder service.
- **Sophos** Standard reporting (building SIEM into next year's integration.

7. Patch Management

- **Barracuda** Energized updates are available for every Barracuda product
- **BitDefender** Bitdefender's GravityZone platform is scheduled to receive patch management features in October, 2017. It will allows for patching of both OS and popular applications.
- **FortiNet** FortiClient can enforce patching of systems as part of compliance. FortiSIEM can also hold configuration data and display the difference between various configurations (potentially if a malicious insider were to make a change that would open a hole, for example).
- **Panda Security** provided by the Systems Management feature.
- **Sophos** Some products have a lite version of patch management but not their specialty.

9. External Audits

- **Barracuda** BVM (Barracuda Vulnerability Manager) can be ran against the customer's website to identify issues that need to be secured. The results can be imported to the Web Application Filter (if purchased) and issues can be remediated with the click of a button.
- **FortiNet** FortiSIEM also has built-in compliance reports, among others, so you can actually schedule those reports to run and send directly to whoever your auditor would be. FortiAnalyzer can also generate custom reports using SQL queries based on historical log data. FortiOS 5.6 (Forti Gate's new firmware) also has a security fabric audit feature built in, where it scans your configuration and makes recommendations for changes.
- **Palo Alto** do SLRs and Posture Assessments with our partners which would be two options for reviewing coverage. If the customer needs a more formal one then our partners normally perform this
- **Panda Security** can fully deliver to evaluate at the endpoint layer with Adaptive Defense. Its agent can be deployed alongside any existing end point antivirus solution to generate insights into application and network activity, as well as to provide any malware attack alerts and forensics in case they occur. All unintrusively through an "audit" observe-and-record implementation mode

10. Security Training

- **Barracuda** Barracuda Campus web site has the latest training materials, videos on demand, recorded webinars and seminars.
- **BitDefender** Bitdefender provides training on its own products
- **FortiNet** product-specific training in the form of the NSE certification program
- **Palo Alto** Disti or partner provides training
- **Panda Security** online training academy (eCampus) is focused on specific product training and deployment practices. Courses can be made available per request to end users
- **Sophos** Training offered around the Sophos solutions.

Current Cyber Security Risks

11. DDOS (Denial of Service (DoS) attacks)

- **Barracuda** Barracuda can validate incoming users with CAPTHCHAs to differentiate between a live person and a bot. The DDOS policy also features an Evaluate Client option that will monitor a client's traffic by embedding JavaScript challenges and monitoring the number of replies with embedded JavaScript Challenge Answers.
- **FortiNet** FortiDDOS protects from both known and zero day attacks with very low latency.
- **Palo Alto** The DoS protection profiles allow you to control the number of sessions between interfaces, zones, addresses and countries based on aggregate sessions or source and/or destination IP addresses. Palo Alto protects against Flood and Resource attacks.
- **Sophos** DoS & Spoof Protection options allow you to set Packet and Burst rates and drops the excessive packets above the set threshold. Intrusion Prevention Policies can be configured to drop packets that match any of the DDoS signatures.

12. Phishing

- **Barracuda** Effective sandboxing and advanced persistent threat prevention should be able to block malware before it ever reaches the corporate mail server. The second layer is anti-phishing protection. Advanced phishing engines with Link Protection look for links to websites that contain malicious code. Links to these compromised websites are blocked, even if those links are buried within the contents of a document
- **BitDefender** BitDefender Safepay offers a secured browser for financial transactions and BitDefender AntiPhishing protects user's private information
- **FortiNet** Advanced Threat Protection tracks known phishing websites and blocks access. FortiNet also offers sandboxing to test suspicious files or attachments to emails.
- **Palo Alto** PA partnered with Proofpoint to provide an email gateway, to scan for malicious emails. Wildfire subscriptions track and block Phishing websites.
- **Panda Security** offers AntiPhishing protection
- **Sophos Cloud** based Email Security for Advanced Threats filters against Spam and Phishing and Malware