## WATCHGUARD

- Long-time provider of email security with large customer base
- XCS 170, 370 and 570 appliances integrate bi-directional email threat protection and data loss prevention on a single platform.
- XCS leverages ReputationAuthority (next-generation reputation service) as a first line of defense to block over 98% of spam and threats at the perimeter BEFORE it enters the network (included at no extra cost).
- XCS deploys a defense-in-depth approach to spam, virus, and threat prevention (including blended threats).
- XCS provides the ability to centrally manage email security from a single point of administration
- XCS 170, 370 and 570 appliances provide multiple layers of redundancy including clustering, patented queue replication, and geographical redundancy (centralized management).

## BARRACUDA

- Barracuda provides content security appliances that are easy to use and affordable to protect organizations from email, Web and IM threats.
- They claim that their products can be up and running in 15 minutes and require no IT expertise.
- Pricing is structured in such a way that they can claim not to charge user/server/port/feature fees.
- In short, their claim to fame is that they are the most affordable solution in the market.

### Key Sales Pitch

<table>
<thead>
<tr>
<th>WATCHGUARD</th>
<th>BARRACUDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Installation is not as simple as they claim with no install wizard available for system setup.</td>
<td>• Barracuda's claim to be &quot;affordable&quot; means cheap. Ultimately, a customer gets what they pay for. Barracuda appliances can be priced so low because their technology is almost all Open Source, meaning they have no intellectual property.</td>
</tr>
<tr>
<td>• These appliance models are built on the same enterprise-class email threat prevention of the higher end XCS enterprise models and include the WatchGuard XCS defense-in-depth protection built on its proprietary 15+ year proven technology.</td>
<td>• Their reliance on Open Source technology creates a high degree of instability and security gaps.</td>
</tr>
<tr>
<td>• Installation and management of XCS appliances is simple and intuitive featuring a web-based GUI. Administrators or small business owners simply set it and forget it.</td>
<td>• In addition, Barracuda uses extremely cheap components in their appliances, resulting in a high percentage of defects on arrival, as well as a high failure rate in the field.</td>
</tr>
<tr>
<td>• WatchGuard XCS 170, 370 and 570 appliances have been specifically designed for small to medium businesses to protect from email threats and prevent outbound data loss at an affordable price.</td>
<td>• Installation is not as simple as they claim with no install wizard available for system setup.</td>
</tr>
</tbody>
</table>

### Truth Behind the Pitch

- Barracuda's claim to be "affordable" means cheap. Ultimately, a customer gets what they pay for. Barracuda appliances can be priced so low because their technology is almost all Open Source, meaning they have no intellectual property.
- Their reliance on Open Source technology creates a high degree of instability and security gaps.
- In addition, Barracuda uses extremely cheap components in their appliances, resulting in a high percentage of defects on arrival, as well as a high failure rate in the field.
- Installation is not as simple as they claim with no install wizard available for system setup.
### WatchGuard vs. Barracuda

#### Performance
- **WatchGuard**: XCS delivers the highest performance in the industry, a fact that is constantly being demonstrated in head-to-head competitive situations where real-world messages are being processed and delivered.
- XCS has been specifically architected to eliminate the processing bottlenecks that plague our competitors.
- Performance is enhanced by including ReputationAuthority, WatchGuard’s next-generation reputation service, which eliminates more than 98% of all inbound threats at the connection level. When Barracuda Central has been evaluated against ReputationAuthority in the field, customers have been shocked at the differences in the levels of granularity and intelligence between the two reputation services.

- **Barracuda**: Barracuda is an SMB play and can only handle small volumes of users and traffic. Their mail systems can’t handle the high-volume mail loads of an organization with thousands of users or those with significant throughput environments.
- Barracuda solutions are sold by functionality, so low-end models have substantially less capability. Important features such as LDAP access, end-user controls, and spam quarantines are not available, forcing users to move up to more expensive systems just to get the basic functionality that their businesses need. To get a fully-functional Barracuda system, a user would have to pay approximately $10,000 for a properly equipped Model 600. Customers report having to run 4 or 5 of the largest Barracuda appliances to handle the mail load that a single XCS appliance processes.
- Barracuda launched a 1st generation reputation service, Barracuda Central, whose effectiveness is highly questionable.
- Barracuda uses extremely cheap components in their appliances, resulting in a high DOA and high failure rate in the field.

#### WatchGuard Competitive Brief

**Competitor: Barracuda Networks**

### WATCHGUARD
- WatchGuard XCS does not rely on open source technology - rather, it is built on proprietary technology with over 15 years proven history.
- WatchGuard XCS deploys a defense-in-depth approach with multiple layers of enterprise-class protection, providing the strongest security at the most affordable price.
- Policies can be set by individual, group or domain, creating stronger, more flexible security, as well as reducing administrative costs.
- XCS 170, 370 and 570 appliances provide bi-directional email protection on a single, easy-to-use platform, unifying administration, policy management and reporting to greatly reduce the costs and administrative burdens of managing multiple appliances.

### BARRACUDA
- Since Barracuda appliances are built on open source technology, their appliances are the poorest quality in the market.
- Not only does Barracuda require separate boxes to handle inbound threat prevention and limited outbound data loss prevention, but each email box functions in its own administrative silo.
- While they claim that their email product handles inbound and outbound email on a single box, their product does not support different settings for bi-directional traffic (i.e. inbound and outbound settings must be exactly the same). For example, you cannot configure a single box to allow executables to be sent but not received. This is also an example of how their policy mechanism is very limited in function.

### Key Sales Pitch Against

- XCS delivers the highest performance in the industry, a fact that is constantly being demonstrated in head-to-head competitive situations where real-world messages are being processed and delivered.
- XCS has been specifically architected to eliminate the processing bottlenecks that plague our competitors.
- Performance is enhanced by including ReputationAuthority, WatchGuard’s next-generation reputation service, which eliminates more than 98% of all inbound threats at the connection level. When Barracuda Central has been evaluated against ReputationAuthority in the field, customers have been shocked at the differences in the levels of granularity and intelligence between the two reputation services.
- Barracuda is an SMB play and can only handle small volumes of users and traffic. Their mail systems can’t handle the high-volume mail loads of an organization with thousands of users or those with significant throughput environments.
- Barracuda solutions are sold by functionality, so low-end models have substantially less capability. Important features such as LDAP access, end-user controls, and spam quarantines are not available, forcing users to move up to more expensive systems just to get the basic functionality that their businesses need. To get a fully-functional Barracuda system, a user would have to pay approximately $10,000 for a properly equipped Model 600. Customers report having to run 4 or 5 of the largest Barracuda appliances to handle the mail load that a single XCS appliance processes.
- Barracuda launched a 1st generation reputation service, Barracuda Central, whose effectiveness is highly questionable.
- Barracuda uses extremely cheap components in their appliances, resulting in a high DOA and high failure rate in the field.
### WatchGuard

- WatchGuard XCS uses a multi-layered approach to spam detection.
- First layer of spam prevention is the WatchGuard ReputationAuthority, the only next-generation reputation system. ReputationAuthority works in real time and makes its decisions based on content (including attachments), volumes, and IP behavior analysis. ReputationAuthority rejects more than 98% of unwanted traffic and threats at the connection-level, with only 1 in 1,000,000 false positives. This eliminates the need for the WatchGuard XCS to scan this traffic, improving performance and reducing bottlenecks.
- Second layer of spam prevention is the Intercept™ engine, the industry's most effective and mature anti-spam technology (almost a decade of proven anti-spam experience). Intercept Anti-Spam provides a solutions-based approach where each Anti-Spam component, when enabled, provides input to the final spam score of a message. Intercept can combine the results of several Anti-Spam components to provide a better informed decision on whether a message is spam or legitimate mail while minimizing false positives. Information retrieved by all of the enabled Anti-Spam components results in a more informed decision on whether the message is in fact spam or legitimate mail. Intercept is able to detect spam in any language and is the only product on the market with a patented approach for detecting image spam.
- XCS features Attachment Content Scanning capabilities for both inbound and outbound email messaging. Message attachments are scanned for blocked or offensive content, viruses, spam content, confidential information, policy violations, or other threats. If there is a problem, the system can perform a variety of actions, such as sending the message to the quarantine area. Attachments can also be stripped, and then the message will continue to be processed by other message checks.

### Barracuda

- Barracuda uses the open source SpamAssassin engine, which spammers are known to reverse-engineer in order to bypass its detection.
- Barracuda requires administrators to constantly adjust and add new scanning rules to catch spam that their engine misses, resulting in high administrative overhead and often also increases the already-high false positive rate.
- Barracuda has features that permit attachment stripping, footer stamping, and body and header keyword search and markets this feature as a highly effective spam detection tool. In reality, however, their spam detection offers no provision for even simple logic in filters or the ability to combine multiple actions on messages which results in legitimate messages being blocked.
- Although they have introduced a 1st generation (at best) reputation service, it relies simply on RBLs that provide a yes/no kind of result. Depending on how aggressive the customer is on their spam threshold, they will either get a low catch rate or a high false positive rate.
- Barracuda does not offer Attachment Content Scanning, which in turn creates security gaps for inbound threats and outbound data loss.
WatchGuard Competitive Brief  
Competitor: Barracuda Networks

**WATCHGUARD**

- **FALSE POSITIVES**
  - WatchGuard XCS provides the lowest false-positive rate on the market, as demonstrated in our head-to-head competitive opportunities.
  - Since ReputationAuthority, the only next-generation reputation system, makes decisions based on content, volume, and behavior, it produces an extremely low false positive rate.
  - XCS’s Intercept engine uses knowledge-based intelligence to learn from messages being passed through the system to make decisions regardless of language and to recognize new spam threats and legitimate email.
  - As a result, XCS provides a 99.999% spam capture rate with 1 in 1,000,000 false positives.

- **VIRUS PROTECTION**
  - WatchGuard XCS provides a multi-layered approach to virus protection.
  - First layer of defense is ReputationAuthority which drops all connections from known virus senders. Only ReputationAuthority tracks the IP address, domain and email address of virus, malformed message, and suspect attachment senders.
  - Second layer of defense is the WatchGuard Threat Outbreak Control, the only automated system that pulls threat information in real-time from ReputationAuthority to provide zero-hour protection by quarantining suspicious payloads. Potential threats are quarantined and then rescanned when new AV signatures are available.
  - Third layer of virus defense include the two most effective anti-virus solutions on the market, powered by Kaspersky and McAfee, both of which have consistently rated 1st and 2nd in response time for providing AV signatures for new and emerging threats.

**BARRACUDA**

- **FALSE POSITIVES**
  - Barracuda has an unacceptably high false positive rate (1 in 10,000 messages as they indicate in their own sales guide), compared to 1 in 1,000,000 for WatchGuard XCS.
  - When Barracuda customers add new rules to catch spam, the false positive rate is further increased.
  - False positives mean legitimate emails are not getting through. This leads to wasted employee time, increased help desk calls to track down missing messages, and potentially lost business opportunities.

- **VIRUS PROTECTION**
  - Barracuda has materially weaker virus outbreak protection and relies on Anti-Virus signatures from the open source ClamAV project. New virus signatures have to be written, tested, and distributed by volunteers, and since they are manually created, they have been known to significantly delay protection. There have been issues where broken virus signatures were distributed to customers that resulted in a complete shut-down of mail processing by Barracuda appliances.
  - Barracuda has a known weakness with regards to directory harvest attacks. Although Barracuda can validate recipients against LDAP, they do not tarpit the attackers because they can only reject on unknown recipient (ROUR). Although they may block detected traffic, they cannot stop the IP from continuing to connect and clogs the network. In contrast, WatchGuard XCS has the ability to block the IP at the connection level upon detection of a directory harvest attack.
**WatchGuard Competitive Brief**
**Competitor: Barracuda Networks**

**WATCHGUARD**

- XCS provides sophisticated built-in content filtering capabilities with integrated, on-box email encryption to prevent data loss.
- XCS provides deep inspection of content, context, sender and recipient information, and communication medium (i.e. how and where it is being sent) of all messages and attachments.
- XCS policies can be set for groups or individuals to provide flexibility based on job function. This can be done on all XCS models. Barracuda cannot apply user-based settings unless the customer purchases a 300 or higher model. Barracuda requires a customer to purchase a 400 or higher model if they wish to do domain-based settings.
- XCS applies instant-on remediation of detected policy violations (including add-on email encryption if so desired) for transparent protection based on user-defined policies.
- XCS includes predefined financial and medical dictionaries for regulatory compliance.
- XCS features document fingerprinting for classifying all types of data files deemed sensitive or confidential, thereby training XCS on what to look for and actions to take upon discovery of such data in outbound communications.
- Unlike Barracuda, XCS does not require a separate appliance to handle outbound data loss prevention. Bi-directional protection is handled from the same appliance, hence providing consolidated security, single point of administration, and eliminates data loss gaps.

**BARRACUDA**

- Barracuda requires a separate appliance, the Barracuda Spam Firewall-Outbound, for advanced outbound filtering, doubling the cost if a customer requires bi-directional protection or data loss prevention, and its DLP capabilities are limited at that.
- They do not position themselves as providing data loss prevention and even if you visit their website, their outbound content filtering capabilities are buried.
- In fact, most of their outbound protection is for virus and spam proliferation.
- Barracuda’s policy configurations are applied system-wide, with no ability to configure different policies for different user groups unless a customer purchases a 300 or higher model (which can do user-based policies), or a 400 or higher model (which can do domain-based policies).
- Barracuda enforces corporate policies by scanning footer attachments, keyword blocking/quarantine, regular expression blocking, attachment blocking based on attachment type, as well as rules that must be created by the administrator.
- Barracuda does offer rules for credit card, SSN, and some privacy regulations, but their out-of-the-box offerings are very limited and require much tweaking by the administrator.
**WatchGuard Competitive Brief**

**Competitor: Barracuda Networks**

---

**WATCHGUARD**

- All WatchGuard XCS appliances provide an intuitive and easy-to-use Web-based management UI that is designed using the same principals as the Microsoft Ribbon UI. All administrative and configuration tasks are performed through this browser-based interface.
- XCS appliances provide on-demand zero-admin clustering for unparalleled capacity and performance creating a large virtual machine that can handle even the most demanding messaging loads, without losing a single message.
- All systems are managed through a single point of access and all configurations are automatically replicated across all systems.
- XCS also provides centralized management to extend policies globally to systems located anywhere in the world.

---

**BARRACUDA**

- Barracuda’s mail policy configurations such as spam handling, attachment-stripping, and footer stamping are applied system-wide, with no ability to configure different policies for different user groups unless a customer purchases a 400 or higher model 400 (which can do domain-based policies), or a 600 or higher model (which can do user-based policies).
- Administrators of Barracuda appliances can’t create business-specific overrides for different users, and that all security is limited to the “least common denominator” for protection unless upgrading to a higher model.
- In addition, Barracuda customers have reported that Barracuda appliances feature a poorly organized UI that is not intuitive and requires many unnecessary steps to perform a simple function. This can be a significant productivity drain on administrators or small business owners who are increasingly under pressure to improve efficiency.

---

**REDUNDANCY**

- WG XCS 170, 370 and 570 models offer multiple layers of redundancy, including:
  - message-level redundancy so you never lose a message patented queue replication capabilities
  - clustering with the ability to replicate configuration across all systems
  - geographical redundancy so customers can centrally manage geographically dispersed systems and apply policies from a single point of administration.

- Barracuda does not offer message-level redundancy on any of its boxes. This technology is unique to the WatchGuard XCS appliances and is a key differentiator.
- Barracuda, does, however, offer clustering and centralized management in its 400 or higher models.
<table>
<thead>
<tr>
<th>WATCHGUARD</th>
<th>BARRACUDA</th>
</tr>
</thead>
</table>
| • All XCS appliances are pre-configured with a series of out-of-the-box, commonly used, detailed reports.  
• Reports are integrated and provide a detailed snapshot of messaging events, ranging from traffic details to system health.  
• Reports can be saved locally or exported for audit purposes, and can be customized and run by domain, group, feature, or time-based.  
• Reports can be run in real-time or can span a lengthy period of time depending on requirements.  
• Reports provide system and content level visibility to message traffic such as policy diagnostics, policy violations, top senders/recipient, top violators (inbound and outbound), compliance/DLP report, system processes used, disposition of messages, viruses, etc.  
• Reports are available that provide visibility into policy compliance, as well.  
• No separate management console is required, and there is no additional fee for detailed reporting. | • Barracuda has only a basic set of simplistic reports, with no support for centralized reporting or message tracking across multiple appliances.  
• Their high level mail statistics are primitive and do not give a complete snapshot of the state of the mail system. Contrast this with the WatchGuard XCS UI where customers will find many useful features including detailed high level summaries, detailed information on incoming mail and outgoing mail and policy violations, and quickly exportable report tabs. |
### WatchGuard

- WatchGuard offers three distinct support programs:
  - LiveSecurity Standard (XCS 170 & 370)
  - LiveSecurity Plus (XCS 570, 770, 970 & 1170)
  - LiveSecurity Gold (upgrade at an additional cost)

- XCS 170 and 370 appliances come with LiveSecurity Standard Support and can be upgraded to LiveSecurity Plus at an additional cost.

- XCS 570, 770, 970 and 1170 appliances come with LiveSecurity Plus Support and can be upgraded to LiveSecurity Gold at an additional cost.

- All programs offer:
  - 24x7x365 telephone access to Customer Support Engineers (except Standard support – only 12x5 support)
  - After-hours support (except Standard – additional cost for this service)
  - Remote installation services (fee-based)
  - Access to online Support Portal including release notes, security alerts, software updates and patches
  - Access to online Customer Portal including product documentation/guides, training materials, My Products Management Center, moderated customer forum
  - Advanced hardware replacement warranty

- LiveSecurity Gold Support is an additional cost and offers additional benefits of:
  - Unlimited support incidents (Standard and Plus programs provide 5 support incidents per year with ability to upgrade to additional 3-incident package)

- Ticket management is available as follows:
  - Web: submitted via Support Portal
  - Phone: via global toll-free numbers

### Barracuda

- Barracuda offers three distinct support programs:
  - Basic Support
  - Enhanced Support
  - Premium Support

- Basic support offers:
  - 8x5 telephone access to Customer Support Engineers
  - 24 hour email support
  - Firmware maintenance
  - Customers report there is no priority issue response time or guaranteed SLA
  - Many customers claim they get assistance from online support forums via other users rather than Barracuda support; company is known to delete posts that indicate flaws in the product

- Enhanced Support is an additional cost available for all models and offers all of the benefits of Basic Support, as well as:
  - 24x7 telephone/email access to Support Engineers
  - Priority escalation to resolve critical issues
  - Data migration of Barracuda unit(s)
  - Hard disk (RAID) replacement

- Premium Support is an additional cost available only for models 6xx and above and includes all of the benefits of Basic and Enhanced Support, as well as:
  - Service Level Agreements (SLA’s)
  - Dedicated Acct. Mgr. and Support Engineers that are familiar with customer environment and Barracuda implementation
  - Dedicated email address for low priority support requests
  - Proactive monitoring for optimal performance
  - Configuration review and weekly issues update
  - Fast-track enhancements via Software Customization

- Ticket management is available as follows:
  - Web: submitted via Support Portal
  - Email: sent to dedicated customer support email address
  - Phone: via global toll-free numbers