Barracuda

Total Threat Protection

Whitepaper

Organizations Are Caught Between a Growing Threat Landscape and Resource Limitations

Today's organizations continue to struggle with providing adequate protection in an evolving threat landscape. Modern threats are sophisticated, difficult to detect, and easily scalable. Furthermore, as network resources become more interconnected, security breaches have a much greater and longer-lasting impact.

Most organizations operate with a common set of network resources that enable users, data, and applications to interact. These same resources create opportunities for threats to breach an organization, also known as network threat vectors. The major network threat vectors are: the network perimeter, the email infrastructure, web applications, web browsing activity, remote access, and mobile devices. Despite the overwhelming diversity of cyber threats that exist, most attacks primarily target these threat vectors.

To complicate matters, adoption of virtualization or public cloud infrastructures have led organizations to rethink their deployment strategies. This means organizations not only have to protect their physical networks, but their virtual and cloud-based resources as well; thereby increasing their overall attack surface.

Unfortunately, most mid-market companies have limited resources to secure all of their threat vectors across these different attack surfaces. Existing staff are stretched thin, often having to deal with many different product interfaces and inconsistent support experiences from multiple vendors. Limited budgets also make it difficult to acquire all of the technology necessary to provide a comprehensive security strategy. As a result, companies often leave one or more of these critical threat vectors unguarded, putting the organization at risk.

Trends Impacting Organizations' Security Posture

Cloud: Organizations are migrating to public cloud services for a number of reasons – with the primary drivers being cost, performance, scalability, elasticity, and ease of deployment. However, this migration also brings with it a unique set of security, accessibility, and data privacy challenges. As organizations move from hosting their own on-premises applications (such as email, CRM) to utilizing cloud services (such as Office 365, Salesforce), they must consider how they can provide adequate accessibility of these resources in the cloud. This requires intelligent traffic optimization and failover at the network gateway to ensure a high-level of availability for these critical applications. Furthermore, as companies leverage the public cloud to host their own application infrastructure, they must also consider the differences in deployment technologies when securing these assets.

Wireless: While wireless networks improve productivity and collaboration in the workforce, they also bring about concerns of end user authentication and visibility. On most wired networks, authentication schemes are straightforward; desktop users authenticate to a domain controller and the authentication events are shared with a security appliance such as a web or network gateway. However, on wireless networks, organizations either allow wireless access without user authentication or they authenticate users on the access point/controller directly. This creates an insecure and inconsistent end-user experience depending on the type of device being used.

Mobility: Mobile devices allow employees to work from anywhere, but it also presents another threat vector where organizations become vulnerable. Laptops, tablets, and smartphones traverse the network boundary with little effort, making the traditional network perimeter borderless. As a result, today's organizations struggle with:

1. Implementing consistent web browsing policies on and off-the-network
2. Providing secure access to corporate resources for remote employees
3. Configuration and management of both corporate and BYOD devices

These challenges are driving new requirements around remote filtering, VPN technology, and mobile device management.

Dispersion: The previous trends discussed above result in increased network dispersion, driving organizations to re-design their architecture to optimize for highly distributed networks. The traditional hub-and-spoke network model was ideal in an environment where most resources (email, web applications, files, etc) were centrally located at headquarters or a primary data center. However, the following trends have quickly made this model outdated:

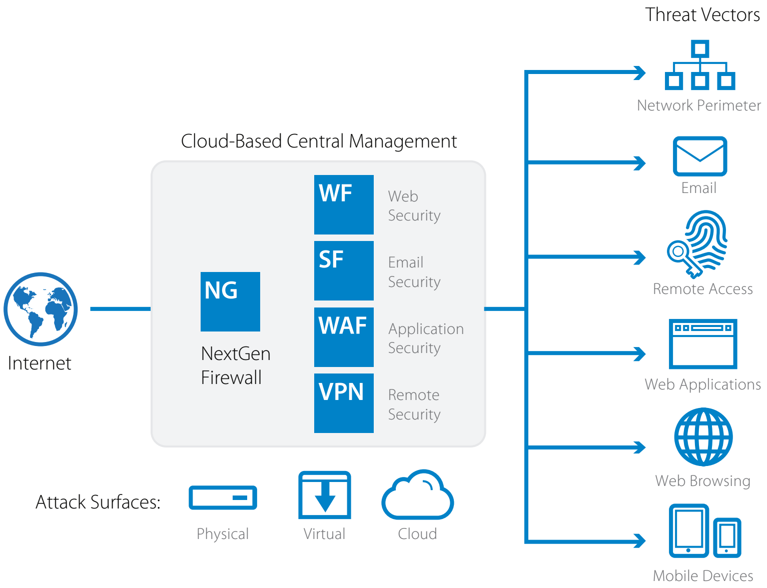
1. Rapid geographic expansion of remote/branch offices
2. Preference of using public cloud services (Software-as-a-Service) over hosting on-premises applications
3. Benefits of deploying infrastructure on public cloud platforms (Infrastructure-as-a-Service)
4. Growing mobile workforce that demands 24x7 access to business-critical resource

In this paradigm, this means moving away from the traditional 'backhauling' of traffic, and instead providing local internet breakouts for remote locations. Organizations should re-design the network architecture to maximize connectivity and maintain operational efficiency while managing a highly dispersed environment.

The Solution is Barracuda Total Threat Protection

Today, administrators need to design a network for optimal connectivity between office locations that are geographically dispersed, employees who are constantly on the move, and a mixture of applications deployed on and off-premises. Furthermore, to secure this network, they should implement their security strategy along the paths where attacks occur.

Total Threat Protection provides a framework for comprehensive, real-time protection that is the key to securing all of your network threat vectors, while providing flexible deployment options to cover your growing attack surfaces. It also offers a consistent set of user interfaces and central management tools to improve operational efficiencies.



Safeguard Networks against Today's Intrusions, Optimize Connectivity, and Provide Secure Remote Access

Barracuda Next-Generation Firewall Family: Barracuda next-generation firewalls are designed to protect the network perimeter, optimize connectivity, and simplify the administration of network operations. They incorporate industry-leading centralized management capabilities with a comprehensive set of next-generation firewall technologies, including:

1. Application & user awareness
2. Intrusion prevention and detection
3. Anti-malware and anti-virus scanning
4. Web filtering & SSL inspection
5. Network access control

With Barracuda's Firewall Family, organizations will find it easy to simplify the investment in network security while improving the performance, availability, and security of distributed networks.

Barracuda SSL VPN: Today's organizations require a flexible, reliable, and secure vehicle for connecting to internal business applications, information, and network resources. An organization's users should be able to connect from anywhere in the world, at any time, from any suitable device. Available as a hardware or virtual appliance, the Barracuda SSL VPN provides the security and connectivity to deliver this access via a simple web browser.

Protect Users from Web and Email Threats

Barracuda Web Security: Barracuda Web Security solutions protect organizations against exposure to web-based malware and viruses, lost user productivity, and misused bandwidth. As a comprehensive solution, they unite multiple layers of spyware, malware, and virus protection with a powerful web filtering policy and reporting engine. Advanced features ensure that organizations adapt to emerging requirements like wireless security, social-network regulation, remote filtering, and visibility into SSL-encrypted traffic.

Companies can choose to deploy Barracuda Web Security solutions as hardware and virtual appliances, as well as a cloud service.

Barracuda Email Security: Barracuda Email Security solutions inspect all email traffic to protect organizations from email-borne threats and sensitive data leaks. Organizations have a variety of data loss prevention and encryption options, as well as granular bulk email management policies. The solution also provides email continuity through message spooling if mail servers become unavailable.

In addition to the on-premises form factors, companies looking for hosted email security can also deploy the Barracuda Email Security Service, a perfect complement to organizations utilizing cloud-based email services such as Office 365. Barracuda Email Security Service provides a layered approach to protecting your email investment with better spam & virus accuracy, real-time threat detection, and granular email management capabilities.

Protect Web Applications

Barracuda Web Application Firewall: Having secured thousands of production applications against more than 11 billion attacks, the Barracuda Web Application Firewall is the ideal solution for organizations looking to protect their web applications from data breaches and defacement. Even without waiting for clean code or knowing how an application works, administrators can rest assured knowing that they have the proper security in place.

The Web Application Firewall is available as a hardware and virtual appliance. For organization looking to secure workloads in the public cloud, it can also be deployed on platforms such as Amazon Web Services (AWS) and Microsoft Azure.

The Barracuda Difference

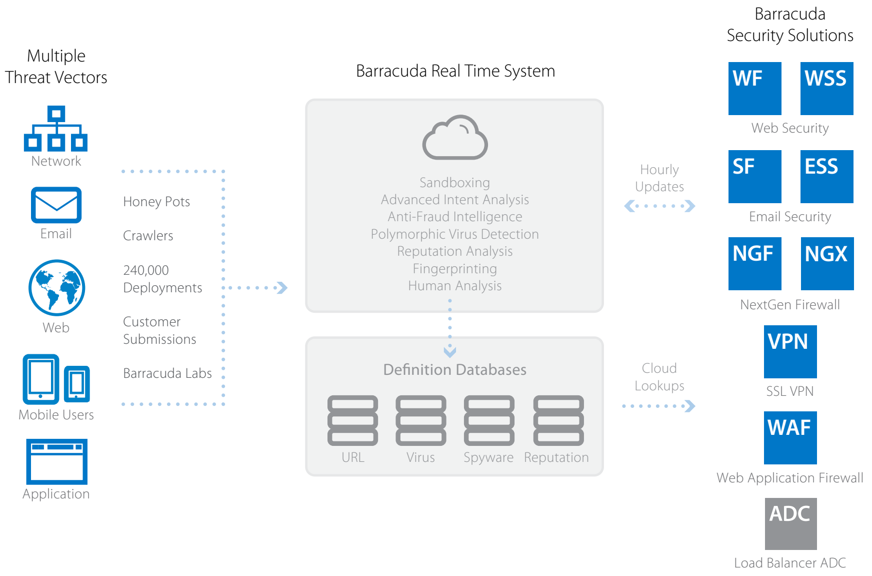
Barracuda Total Threat Protection is an ideal security framework for IT professionals who wear many hats and organizations that contend with resource and budget constraints. Additionally, customers will also benefit from:

Common Interfaces: Barracuda's award-winning solutions share a common, intuitive interface for a familiar and consistent user experience. This makes it easy for small and medium-sized organizations to implement and manage their security solutions with minimal overhead.

Centralized Management: Our security solutions can be managed from a "single pane of glass". With our award-winning central management tools, administrators have a complete view of their security posture, from configuring policies to running reports, and much more.

Award-winning Customer Support: Barracuda's award-winning technical support teams are always available whenever you need assistance—24/7, 365 days a year.

Threat Intelligence: All Barracuda solutions are backed by Barracuda Threat Intelligence, a powerful security framework that combines threat data collection from multiple sources around the world, advanced analysis and research, and a global operations network that supports gateway defense, end-point security, and real-time protection through the cloud. The framework is designed to provide comprehensive, timely, up-to-date threat protection across multiple threat vectors while maintaining the highest level of performance for both on-premises solutions and hosted environments.



Conclusion

In providing a comprehensive security approach, administrators should understand the key trends that are driving the requirements in their network design:

1. Cloud-based workloads present new challenges in providing connectivity and security of users, data, and applications
2. Wireless networks bring challenges around implementing a uniform set of policies and workflows for both wired and wireless devices
3. Mobile devices have turned the network perimeter borderless, forcing companies to re-evaluate web filtering and VPN requirements
4. A highly dispersed network of office locations, users, and applications are causing organizations to design networks with multiple internet breakouts instead of the traditional 'backhaul' model.

Once these trends are understood, administrators can implement the appropriate Barracuda security solutions along the main threat vectors that attacks generally target. These are:

- The network perimeter
- Email infrastructure
- Web applications
- Web browsing
- Remote access
- Mobile devices

Furthermore, they must consider how changes in deployment technologies may expand their attack surface – from physical to virtual to cloud-based networks. Finally, a unified management and customer support experience complete Barracuda's Total Threat Protection offering.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

1-408-342-5400
1-888-268-4772 (US & Canada)
info@barracuda.com
barracuda.com