



Secure Application Management with Alteon Application Switch

Solution Brief



Today's most prevalent security threats, such as viruses, worms and denial-of-service (DoS) attacks, exploit vulnerabilities in the application layer of the network. Malicious code is embedded within the content, or payload, of data packets, where it takes advantage of vulnerabilities in the protocols or behavior of applications—such as Web Services, instant messaging, email, FTP or databases—to gain access to network resources or subvert the application.

Ironically, the device most commonly thought of as providing protection against network vulnerabilities—the firewall—has traditionally not been very well suited to protecting networks against application-layer infiltration.

Security must evolve to mitigate new threats

Firewalls were developed so that opening the corporate network to the outside world is not an open invitation for anyone to come in and go anywhere. For example, when a business implemented an email system, it needed to ensure that all incoming traffic was blocked, unless it was headed for the email server and looked like email. Firewalls were based on filtering technology that inspected packet headers, for information such as source and destination addresses, and source and destination ports.

Stateful firewall inspection, a breakthrough of the 1990s, sped up this process by keeping track of the relationship of packets to one another, so that only the first packet in a connected stream had to be inspected. If the first packet was permitted through the firewall, all subsequent packets in that stream could automatically be admitted, thereby improving performance.

However, as businesses have become more dependent on information and communications technology, and the sophistication of network attacks has grown at an exponential rate, this level of protection is no longer sufficient. It misses malware hidden deep within data streams, in packet payloads. To be secure today, your network needs tools to protect the application layer—the level at which the most devastating attacks occur.

How to spot the hidden threat?

Implementing effective application-layer security is fundamental to protecting your business from today's most sophisticated network security threats, but, as we have seen, traditional firewalls are not up to the job. Securing your applications properly requires deep packet inspection: looking beyond packet headers to packet payloads and inspecting every packet, not just the first.

It's not just malicious traffic that is using application-layer vulnerabilities to affect your network. While not traditionally regarded as a security breach, peer-to-peer (P2P) file sharing, which today accounts for as much as 80% of Internet traffic, hogs bandwidth and leaves other network users with poor network performance. To limit the unauthorized use of peer-to-peer applications by your employees, you need to be able to find the signatures of these applications—which reside in the application-layer.

Performance: zero compromise

The real challenge is to perform application-layer inspection without creating bottlenecks in the network. Until recently, the technology simply did not exist to carry out deep packet inspection fast enough to avoid affecting the performance of the associated applications. And you can't afford to have the performance of your applications compromised. Not when staying competitive depends on being fast, agile and responsive. Not when the services that every business will depend on in the future, like voice over IP and real-time collaborative tools, simply won't tolerate delays.

A total approach to application security

To meet this challenge, Radware offers a solution that really works to secure the application-layer of the network, without affecting network performance—indeed, while improving application performance. Our approach to application-layer security is a perfect example of our overall security philosophy:

- Layered Defense—building security into every layer of the network.
- Unified Security Framework—building security into the fabric of your organization: into people, policies and processes -- as well as devices and network layers.
- Open standards and partnerships— working with the wider industry and vendor specialists to identify new security threats and develop effective solutions.

By implementing this approach we are able to offer an application-layer security proposition that will enable you to take full advantage of the most important applications of today and tomorrow, at a lower total cost of ownership.

Defense at every point

In the most simple of terms, network security is about ensuring that every transmission that enters and leaves your network is a legitimate use of network resources, and that non-legitimate traffic neither enters nor leaves. The network perimeter is therefore the most obvious point at which to enforce security, and the firewall is the most obvious perimeter defense mechanism.

While it's vital to provide as much protection as possible at the perimeter, there are three problems with relying only on perimeter protection through firewalls:

- As discussed, firewalls are not traditionally designed to handle the intensive processing required for deep packet inspection.
- Not every threat originates from outside the network: disgruntled employees, unsecured back-door access and infected laptops are also a security risk, and peer-to-peer applications can be wholly internal.
- No perimeter defense should ever be relied on to be 100% effective.

For this reason, Alteon's application-layer security solutions address both the network perimeter and the network core, by building security into the part of the network that is specialized for controlling application traffic: the application switch. The Alteon Application Switch uses ground-breaking technologies to provide 'defense in depth' against the most common application-layer attacks and unauthorized peer-to-peer communication.

Constant security, constant performance: security in the switch

Unlike firewalls, switching technology was developed specifically to inspect packets and direct them with minimal network latency. Application switches switch traffic based on the content of packets at the application layer, while maximizing the performance of the application. So it makes sense to build on these deep packet-inspection capabilities to provide security against illegitimate application-layer traffic, as well as performing the primary function of controlling legitimate application-layer traffic.

The Alteon Application Switch is typically located in close proximity to the applications and data servers it controls in

Why Radware?

Radware is a focused vendor in application delivery, with more than 12 years of experience in developing and supporting application delivery solutions.

The Alteon Application Switches seamlessly work with Radware's advanced application and network security offering, which includes:

- DefensePro - Behavioral-based Intrusion Prevention System (IPS) providing real-time signature protection from zero-day attacks and non-vulnerability threats, as well as DoS protection
- AppWall - Web Application Firewall (WAF) securing Web applications and enabling PCI compliance
- AppXML – Advanced XML & Web Services gateway providing XML firewalling and Web Service security

the data center. Its Intelligent Traffic Management capabilities are the best available, offering inspection, classification, control and reporting functionality, all essential for taking full advantage of new converged applications like instant messaging, VoIP and multimedia.

Combat abuse of resources...

The switch uses a database, pre-populated with a wide range of application and attack signatures, to distinguish legitimate application traffic from illegitimate attack traffic. The database is frequently updated and network administrators can also define freeform application, DoS and virus signatures.

The combination of signature detection and the switch's primary functions of monitoring, directing, filtering, prioritizing, rate-limiting and rate-shaping application traffic, gives the Alteon Application Switch powerful security capabilities, including:

- Identifying and combating high-profile worms and Trojans without stopping the entire application protocol
- Identifying and blocking common DoS attacks such as LandAttack, Smurf Attack, SynFin and many others
- Preventing spyware applications from sending corporate data where it shouldn't be going
- Identifying port-hopping peer-to-peer applications and controlling them by denying their use or limiting the amount of bandwidth they can use
- Protocol-based rate limiting for TCP, UDP and ICMP protocols, to ensure that protocol-based attacks can't flood servers
- Shaping and prioritizing business- critical application traffic to minimize impact on it in the event of a worm attack

...while improving their performance

All of the security capabilities of the Alteon Application Switch are offered in addition to its ability to optimize network use, even to the level of being able to control the amount of bandwidth a single user can apply to a particular application. With advanced load-balancing, application redirection and prioritization functionality, the Alteon Application Switch can:

- Improve server and device utilization and reduce server costs by up to 50%
- Extend network asset life, saving up to 40% annually
- Enable implementation of streaming- media architectures that drive significant ROI through enhanced employee communication and training, without additional travel expenses
- Improve application availability and performance, resulting in better employee productivity and customer satisfaction

The most comprehensive data center security offering

Alteon Application Switches are a key part of Radware's security portfolio, and can be extended to provide customers with the most comprehensive data center security offering.

Web Application Security

Combining Alteon Application Switch with AppWall, Radware's Web Application Firewall (WAF), enables to secure Web applications and to enable PCI compliance by mitigating Web application security threats to prevent data theft and manipulation of sensitive corporate and customer information. Radware's AppWall incorporates advanced, patent-protected Web application security filtering technologies to seamlessly detect threats, block attacks and report events.

Web Services and XML Security Gateway

Deploying Alteon Application Switch along with Radware's Web Services security gateway, AppXML, provides extensive protection for Web Services deployed in an organization. In addition, by enabling interoperability with existing Identity Management Systems in the organization, AppXML enables enterprises to achieve a higher ROI through secure, efficient e-business process integration.

Behavioral-based Intrusion Prevention System

DefensePro, Radware's real-time Intrusion Prevention System (IPS) and DoS-protection device, maintains business continuity by protecting applications against known attacks and emerging network attacks such as non-vulnerability based attacks that misuse the application, zero-minute attacks, SSL attacks and VoIP service misuse – all without blocking legitimate user traffic and with no need for human intervention.

Want to know more?

If you'd like to learn more about how Radware can help you secure your network against application-layer threats or give you more extensive help with network security visit our Website at www.radwarealteon.com.

About Radware

Radware, the global leader in integrated application delivery solutions, assures the complete availability, performance and security of business-critical applications for nearly 10,000 enterprises and carriers worldwide. With Radware's comprehensive and award-winning suite of products, companies can drive business productivity, improve profitability, and reduce IT operating and infrastructure costs by making their networks "business-smart."

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements - phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

If you'd like to learn more about how Radware can help you secure your network against application-layer threats or give you more extensive help with network security visit our Website at www.radwarealteon.com and at <http://www.radware.com/Solutions/Enterprise/Security/default.aspx>

For information regarding Radware's entire portfolio of application delivery and network security products for business-smart networking, please visit www.radware.com.