

Increasing Profit Margins with Network Security Services

This white paper focuses on helping service providers increase profit margins with highly differentiated network security services, with no upfront investment or dedicated security staff, using Alert Logic's *Network Protection On-Demand* solution.

Contents

Introduction	2
The Opportunity in Security Services	2
Service Provider Trends	3
About Alert Logic.....	4
Threat Manager for Service Providers	6
Service Provider Feature in Threat Manager	6
Deploying Alert Logic in Service Provider Setting.....	7
Appliance Models.....	8
Advanced In-Cloud Deployments .	11
Summary.....	14

Alert Logic, Inc.

1776 Yorktown, 7th Floor, Houston, TX 77056 | 877.484.8383 (toll free) | 713.484.8383 (main) | 713.660.7988 (fax) | www.alertlogic.com

Alert Logic and the Alert Logic logo are trademarks, registered trademarks, or service marks of Alert Logic Inc. All other trademarks listed in this document are the property of their respective owners.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, ALERT LOGIC, INC. PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Alert Logic, Inc., except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Alert Logic, Inc. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Changes or improvements may be made to the software described in this document at any time.

© 2010 Alert Logic, Inc., all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Invision Security and Alert Logic are trademarks or registered trademarks of Alert Logic, Inc. or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Introduction

After several years of explosive growth leading up to the bursting of the technology bubble, the IT industry is again facing another tectonic shift. Advancements in Internet Protocol (IP) communications and the emergence of Software-as-a-Service (SaaS) are driving the next generation business model for telecommunications carriers and web hosting providers, creating opportunities that were not available just a few years ago. As emerging technologies continue to make more sophisticated web enabled applications a reality, service providers that control data center and network infrastructure are beginning to be seen as strategic vendors by IT buyers.

The Opportunity in Security Services

For many businesses, large and small, effectively protecting internal networks from security threats means dealing with complexity and high costs. While perimeter security devices, such as firewalls, and endpoint defenses, such as anti-virus solutions, were once an effective means to manage exposures to attacks and infections, these defenses alone are no longer sufficient to protect internal networks.

Internet worms, unauthorized access attempts, and Trojans originating inside firewalls on internal networks can negatively impact network performance and availability and employee productivity. According to the FBI/CSI Computer Crime and Security Survey, while 97% of organizations deployed firewall and anti-virus protection, more than 52% continue to experience security breaches. On average, companies participating in the FBI/CSI survey reported more than \$200,000 in financial losses, per company, due to security breaches. Because internal networks still face substantial risk, many organizations consider deploying some type of intrusion detection or prevention product to improve the protection of their network. However, many IT managers have learned either from painful first hand experience or from the experience of colleagues in the industry that existing intrusion prevention products come with a myriad of issues:

- They are extremely prone to false alarms.
- They require constant time and attention for effective operation

IT managers who implement existing intrusion prevention products find themselves continually monitoring and managing the product. Reviewing alerts, refining intrusion prevention rules, and fine-tuning the intrusion prevention product to optimize protection levels becomes a never-ending series of tasks. Making an informed buying decision about intrusion prevention products can be overwhelming. Hundreds of security products claim to secure your network from every conceivable risk. However, these security products do not adequately address all of your network security challenges:

- Existing network security products are difficult to manage and costly to deploy and operate.
- Network threats evolve and easily bypass perimeter security solutions, impacting network security and availability.

- Failure to comply with industry regulations for protecting sensitive financial or personal data can lead to fines, litigation, and loss of public trust.

Many businesses are beginning to turn to their service providers for help. While several years ago IT buyers looked to pure play Managed Security Service Providers (MSSP) for relief, today's IT executives expect security to be delivered "in-cloud" by the same service providers that already provide their telecommunications, IT infrastructure outsourcing, and managed application services.

Service Provider Trends

Although Gartner predicted that service providers will become major players in security as early as 2005 in the report titled "**In the Cloud' Security Services Will Change Providers' Landscape**", few providers have delivered true in-cloud security services, instead they have relied upon traditional managed security monitoring solutions that lack innovation and effectiveness. In fact, in a Network Computing test of five security providers in late 2006, all five delivered almost the same level of service differentiated only by price and packaging. The gap between buyer expectations and solutions found in the market is widening, creating opportunities for service providers that understand buying trends of today's enterprises:

- Latest market surveys indicate that while most security solutions are similar in functionality, most fail due to deployment complexities. This trend is driving IT executives to seek solutions that eliminate as much on-premise infrastructure as possible from the equation.
- IT buyers are growing tired of "one size fits all" managed service solutions that force them to hand over all visibility and security decisions to a third party. Astute security managers today want to control how much or how little of their security management they participate in and expect their solutions to adapt to their choices.
- Buyers are becoming increasingly aware of Software as a Service (SaaS) solutions and are beginning to expect highly functional security products to be delivered on-demand.
- Today, regulatory compliance has become even more crucial to enterprises than security. Solutions that provide little to alleviate the pain of meeting compliance mandates stand little chance in capturing their attention.
- Finally, high cost is preventing many enterprises from deploying adequate security deep within their network, where most critical data resides. Despite having economies of scale, service providers have been unable to meet the need for lower price points to significantly impact customer penetration rates.

In-cloud, on-demand security services provide even more benefit to service providers themselves than their customers. Services deployed within the network cloud are not only highly scalable, but cost far less to deploy, administer and upgrade. The move to security in-the-cloud also eliminates the need to provision and support equipment on customer premise, which today is an enormously costly part of many service providers' operations. Most importantly, in-cloud infrastructure can be oversubscribed, providing economies of scale rarely achieved with customer premise equipment.

If the business case for in-cloud security is so clearly defined, why are there virtually no commercially available solutions in existence today? Most of the reasons point to lack of mature solutions that effectively enable on-demand security services:

- While most service providers see security services as an important part of their strategy, more than 50% do not feel that they have the expertise necessary to deploy in-cloud services.
- Few network vendors have introduced in-cloud products. Although large infrastructure players have announced their intent to be in this space their solutions are often disruptive and force service providers to perform fork lift infrastructure upgrades.
- None of the solutions on the market provide end users with a rich user experience they expect from SaaS applications, forcing service providers to develop feature limited portals for basic reporting. Not only do these projects take a long time to get off the ground, but they often fail to be truly competitive and gain adequate market traction.
- While SMB and SME buyers have the potential to be the biggest market for in-cloud security services, few products are specifically designed for mid-sized business and small enterprise customers. SMB/SME security products available today are often little more than a scaled down and feature limited version of enterprise solutions, and provide few benefits small businesses truly care about.

Threat Manager for Service Providers

Alert Logic has designed the *Network Protection On-Demand* platform around service provider needs. This solution enables service providers to deliver highly differentiated security products with no up front investment or dedicated security staff.

Alert Logic allows service providers to achieve previously unavailable functionality and price points by combining the benefits of the Software-as-a-Service application architecture with cutting edge technology like the virtualized Multi-Tenant Edition appliances. This allows service providers to deliver fully-managed and highly differentiated network security services at a fraction of the cost of their competitors.

In service provider environments Threat Manager includes three major components:

- Threat Manager User Interface (UI) that provides service providers and their customers a single web console to manage all security functions. This component is hosted by Alert Logic.
- Alert Logic appliances that monitor network attacks, perform vulnerability scans and initiate defensive actions. This component is deployed by service providers on customer premise or within the service provider's network cloud.
- Traffic Director appliances that enable service providers to provision the Threat Manager service in high performance carrier or distributed data center environments.

Alert Logic's SaaS platform allows service providers to develop value-added services using Threat Manager as a platform, such as managed 24/7 security monitoring or vulnerability management services. By utilizing the optional ActiveWatch service, service providers can leverage Alert Logic's Security Operations Center (SOC) to provide 24x7 security monitoring services or choose to augment their security staff after business hours.

The goal of Alert Logic's solution is to enable service providers to reach the broadest possible customer base without incurring heavy costs or introducing sales friction.

Service Provider Features in Threat Manager

Designed from the ground up as a Software-as-a-Service (SaaS) solution, Threat Manager is a service delivery platform that provides all the building blocks necessary to rapidly deploy effective managed security services in the most cost effective manner..

The Threat Manager UI is a single unified web console that allows service provider staff and customers to monitor threats, manage vulnerabilities and report on regulatory compliance across an unlimited number of sites, greatly simplifying security and compliance management tasks. The Threat Manager UI is a rich user web portal built on AJAX technology and extensively field tested for suitability in service provider environments.

As the most critical customer facing component, the Threat Manager UI offers Service Levels of 99.9%. All of the software and infrastructure components of our solution are hosted in our redundant SaS-70 certified data center facilities enabling turnkey deployment and rapid service provisioning.

Unlike solutions developed primarily for enterprise needs, Threat Manager includes a number of service provider centric features that allow Alert Logic partners to:

- Rapidly provision services, on-premise or in-cloud, without introducing complexity into their networks or doing a truck roll on location
- Embed custom logos and color schemes in the Threat Manager UI through branding features.
- Configure Threat Manager with a customized domain name and originate notifications from the service provider's email address
- Provide a common UI for service provider staff and customers, greatly simplifying end user support
- Manage and monitor all customers from a single interface that can be configured and customized for each member on the service provider team
- Create personalized dashboards and reports that can be configured to report on one or many customers in a single view
- Route incident and reporting notifications on a per-customer basis. Threat Manager also includes extensive business unit reporting features, allowing each customer to segment their network into logical zones and host groups
- Delegate user rights to customers to enable self-management or restrict user rights to control the level of access each customer has
- Provision services in high density environments with Multi-Tenant Edition appliances
- Provision services in high bandwidth capacity carrier or distributed data center environments with the Traffic Director appliance

Deploying Alert Logic in a Service Provider Setting

While there is currently no market consensus whether in-cloud or customer premise based solutions will begin to dominate security sales in the future, customers today demand the flexibility to choose the deployment path that suits their environment best.

Alert Logic has designed the *Network Protection On-Demand* architecture to enable service providers to offer both deployment methods to be easily provisioned side by side and in any combination. Alert Logic supports the following deployment models:

- On-premise – dedicated appliances deployed at each customer location, typically on an internal Ethernet switch (CPE deployment)

- In-cloud – dedicated or multi-tenant appliances deployed on the service providers backbone or in the data center facility

With both deployment models the appliances are deployed virtually inline using Ethernet taps or mirror ports on a switch at the network core or distribution segments. The virtual inline deployment path drastically reduces the possibility of network disruption and eliminates the need to install the appliances directly in the network path as is the case with inline IPS products or switch based IPS blades.

This approach greatly simplifies deployment and eliminates the need for service providers to perform forklift upgrades of their existing infrastructure in order to support a new security product. The flexible deployment model offered by Alert Logic appliances also affords the opportunity to greatly increase coverage and provide protection deep within customer networks across the entire enterprise, rather than limited coverage at the network perimeter.

Appliance Models

Alert Logic appliances ship in a shallow depth (14”) 1u form factor designed for standard 19” racks. Each appliance is drop shipped from the Alert Logic distribution facility pre-configured for the customer’s network and require no further configuration.

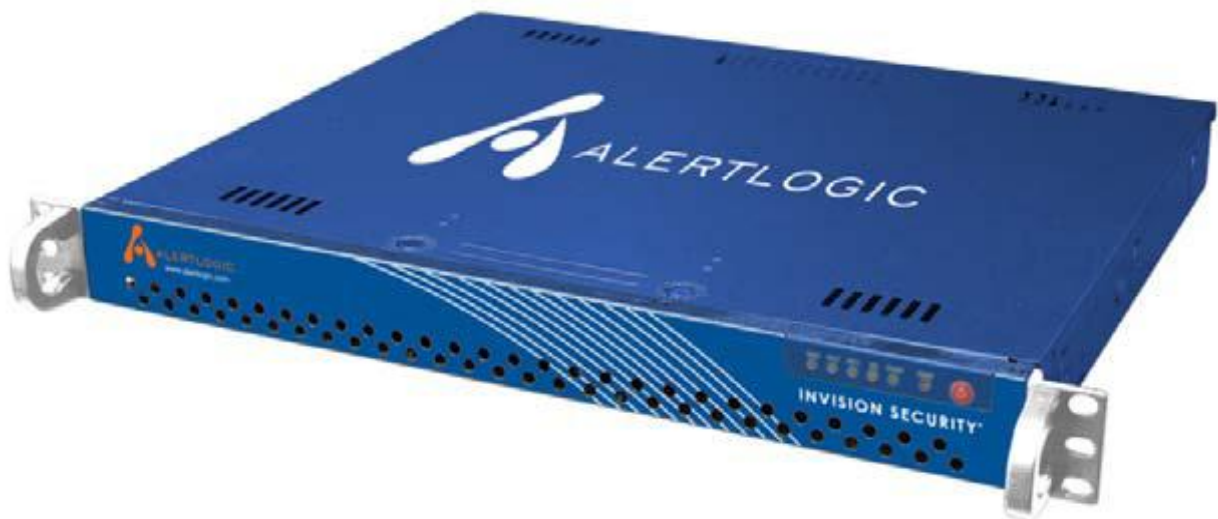


Figure 1: Alert Logic Appliance

In addition to monitoring interfaces, each appliance includes a dedicated managed Ethernet interface used to communicate with the Threat Manager infrastructure at the Alert Logic data center, perform vulnerability scans and issue defensive actions on customer networks.

Note

Communications between the Alert Logic data center and remote customer appliances are encrypted using an AES-256 bit cipher.

Dedicated appliances

Dedicated appliances are the most versatile option, and can be deployed either on customer premise or in-cloud. Although these appliances have up to four monitoring ports, it is a best practice to deploy a dedicated appliance per customer segment when possible.

Dedicated appliances are ideally suited for customers that have bandwidth requirements of between 10Mb to 1Gb. Customers with more than 1Gb in aggregate traffic may need to deploy multiple dedicated appliances and may need to consider leveraging the Traffic Director appliance for networks that carry up to 5Gb.

Each appliance is licensed by the bandwidth capacity and number of nodes the appliance can scan. In most cases appliances can be upgraded with a higher capacity license in the field without the need to replace the appliance.

Model	Bandwidth	Nodes	Monitoring Interfaces
ISE 1540	10 mbps	50	(1) 10/100/1000
ISE 1560	35 mbps	100	(1) 10/100/1000
ISE 2020	60 mbps	250	(1) 10/100/1000
ISE 2040	85 mbps	500	(2) 10/100/1000
ISE 3020	125 mbps	750	(2) 10/100/1000
ISE 3040	250 mbps	1,000	(4) 10/100/1000
ISE 5040	500 mbps	2,000	(2) 10/100/1000
ISE 5060	1 gbps	2,000	(4) 10/100/1000

Figure 2: Dedicated Appliance Models

Multi-Tenant Edition (MTE) Appliances

Service providers that build security solutions for the SMB market face a number of unique challenges:

- Very few viable solutions exist today for in-cloud security services. Several vendors are beginning to introduce in-cloud products, but they often force costly infrastructure upgrades.
- In data center environments, deploying dedicated appliances for small customers often results in prohibitively low customer densities per rack, making security services for SMBs economically unfeasible.

- Price points of commercial SMB products fail to deliver adequate profit margins when on-premise installations and ongoing management overhead is factored into the overall cost.

Alert Logic has designed the MTE appliance family specifically for the needs of web hosting, network and telecommunications providers. These appliances enable service providers to deliver turnkey, high margin security services for SMBs deep within their networks, including data center facilities, carrier backbone links and ISP Points of Presence (POPs).

Multi-Tenant Edition appliances have been designed using Alert Logic’s proprietary virtualization technology that enables service providers to host up to 50 customers on a single physical appliance unit. Customer density achieved with this design has numerous benefits enabling service providers to:

- Achieve very low price points to achieve maximum SMB market penetration, while maintaining healthy profit margins that exceed those of solutions built in-house.
- Significantly reduce data center and power consumption per customer costs.
- Eliminate provisioning costs associated with truck rolls to customer premises.
- Reduce ongoing costs associated with monitoring and managing multiple appliances deployed on customer premises.

MTE appliances are extremely easy to install on service provider networks by simply mirroring or tapping the traffic on target segments.

Once installed, the unit can be rapidly provisioned for new clients on demand. Alert Logic’s staff will perform most of the necessary provisioning tasks, making the process as simple and cost effective as possible. Each virtual tenant instance will receive only the traffic for the address space it is configured to inspect, whether it be a single host or an entire network segment.

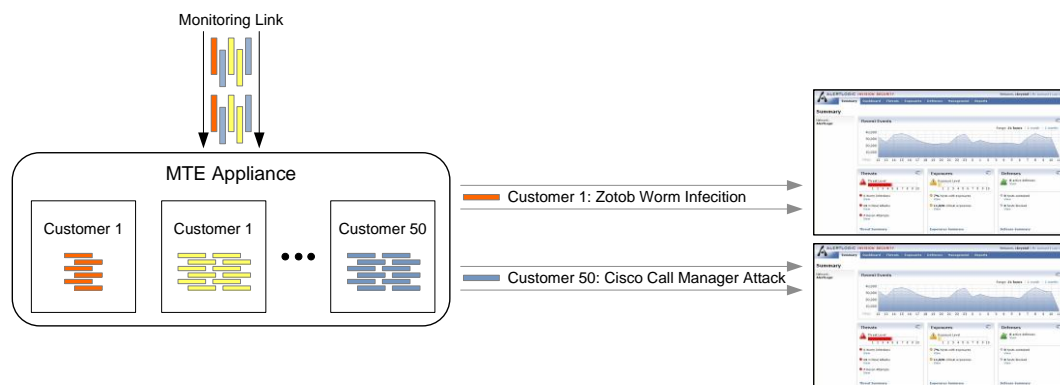


Figure 3: MTE Appliance Data Flow

MTE appliances were specifically designed for the SMB market, where customers tend to use less than 5Mb of traffic. Each MTE tenant instance can withstand up to 50% bandwidth overrun without packet loss.

Alert Logic provides constant monitoring of bandwidth utilization per client and will notify the service provider when an MTE tenant begins to exceed their allotted bandwidth and needs to be upgraded to a dedicated appliance. Customers that have outgrown the MTE appliance can easily be transitioned to one of Alert Logic’s dedicated appliances without any loss of data or significant interruption in service

Model	Tier	Bandwidth	Tenants
MTE 1100	Tier I	25 mbps	1-5 (up to 5 mbps each)
MTE 1100	Tier II	125 mbps	1-25 (up to 5 mbps each)
MTE 1100	Tier III	250 mbps	1-50 (up to 5 mbps each)

Figure 4: Multi-Tenant Edition Appliance Models

MTE appliances ship on a common hardware platform and can be upgraded in production with a new license without service disruption.

MTE appliances have two Gigabit Ethernet monitoring ports and can be configured for copper or fiber gigabit networks. Although MTE appliances are designed for standard data center environments with adequate cooling, Alert Logic can provide pricing for NEBS compliant devices upon special request.

Notes

This solution is designed for in-cloud only deployment and is not offered in on-premise mode.

Due to in-cloud deployment MTE appliances do not provide vulnerability scans. Customers that wish to use internal vulnerability scanning capabilities are advised to use a dedicated appliance in addition to the MTE appliance.

Due to their in-cloud deployment, MTE appliances do not provide internal intrusion protection functions, such as containment and quarantine. MTE appliances can, however, execute firewall blocking actions in most service provider environments.

Advanced In-Cloud Deployments

Large service providers that deliver telecom, network or web hosting services often require specialized in-cloud infrastructure to accommodate the unique requirements of their network environments These unique requirements include:

- Hosting companies with multiple customer VLANs deployed on common switch infrastructure, where the number of customers is significantly greater than the number of monitoring ports available.

- Large datacenters with customers who have logical networks that span multiple switches, equipment racks or cages and need to be monitored in multiple locations simultaneously.
- Network environments that experience asymmetric routing conditions, producing incomplete traffic flows at various monitoring points.
- Telecom and Internet Service Providers that wish to provide in-cloud services to a large number of customers using a common pool of dedicated and MTE Alert Logic appliances deployed at a local POP or other upstream network aggregation point.
- Network links that carry between 1Gb to 5Gb of traffic per monitored segment.

To accommodate these unique requirements, Alert Logic provides the Traffic Director appliance to simplify deployment of security appliances in highly distributed and complex network environments.

The Traffic Director (TD) appliance(s) effectively aggregate(s) up to 5Gb of traffic delivered from multiple mirror ports or tap points. Once network traffic is combined on the Traffic Director appliance the data is then partitioned by customer and redirected to a pool of dedicated or MTE appliances.

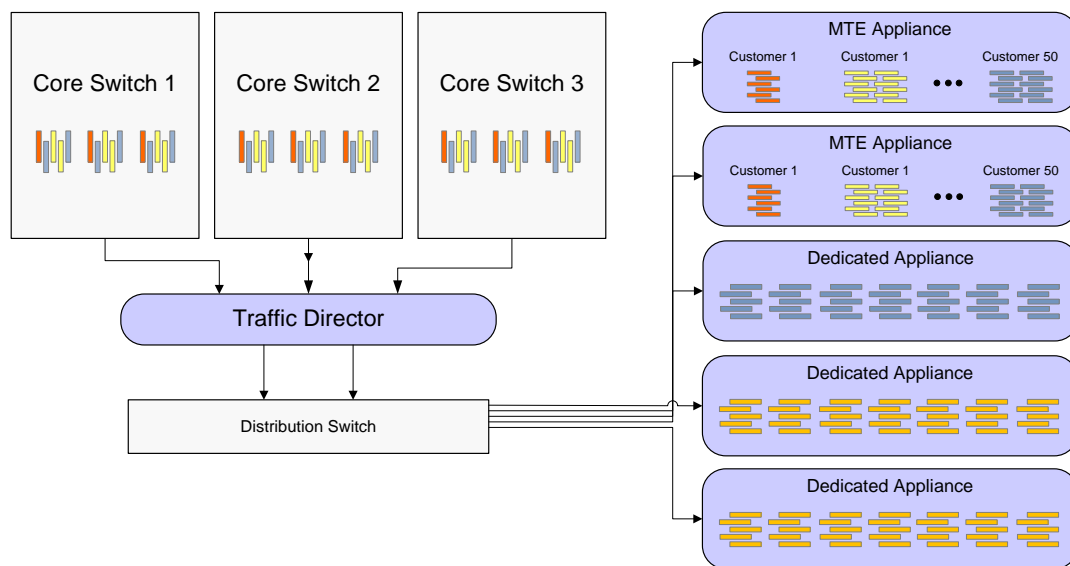


Figure 5: Traffic Director Data Flow

The Traffic Director solution consists of a single appliance that can aggregate multiple incoming ports to deliver up to 5Gb of aggregate throughput. The appliance ships in a 1u form factor and provides up to 6 Gigabit Ethernet interfaces in either copper or fiber ports. Any of the 6 ports may be used as input or output ports.

Network traffic aggregated on the Traffic Director appliance can be filtered and redirected using one of four methods

- IP address range (most common)
- VLAN id
- Network protocol
- MAC address
-

The Traffic Director redirects the traffic at Layer 2 to an unlimited number of destination appliances by modifying the destination MAC address of all packets. The destination MAC address used by the Traffic Director is typically the assigned MAC address of the dedicated of MTE appliance.

Note

Although Traffic Director appliances are typically designed for up to 5Gb throughput, Alert Logic has developed a specialized architecture for environments that carry 10Gb and beyond. Please contact your Alert Logic representative for a review of your network topology.

Summary

Alert Logic has designed the *Network Protection On-Demand* platform around service provider needs. This solution enables service providers to deliver highly differentiated security products with no upfront investment or dedicated security staff, while achieving previously unattainable price points in the market.

The goal of Alert Logic's *Network Protection On-Demand* solution is to enable service providers to reach the broadest possible customer base without incurring heavy costs or introducing sales friction.

Alert Logic eliminates the high cost and complexity of deploying and managing disparate network security point products by combining the critical elements of internal network security into one seamless on-demand package.

About Alert Logic

Alert Logic's patented solutions are the smartest choice for over-regulated businesses with underfunded IT departments to secure networks and ensure compliance. Its cloud-powered managed solutions combine intrusion protection, vulnerability assessment, log management and 24x7 threat surveillance, and are designed to maximize revenue and profit opportunities for service providers and hosting partners. Enterprises experience a solution that addresses network security and compliance requirements at a low price point, with little dependency on IT resources. Alert Logic is based in Houston, Texas and was founded in 2002. More information about Alert Logic can be found at <http://www.alertlogic.com>.

[CONTACT US](#)