Your business is continuously confronted with different threats and multiple types of attacks, both internal and external, which have great potential to cause disruption and damage to your infrastructure, information, communication technologies and business applications. Organizations that want to avoid negative business impact and reduce risk and exposure must address challenges on various levels – while managing the costs and complexities of securing their businesses.

Risk can present itself in operational challenges, network vulnerabilities and continuously evolving cyberthreats. In order to reduce exposure to risk, it is critical to have an in-depth, layered approach to predict, detect, alert and respond to threats that allow security-impacting events to be anticipated and corrective action taken before they impact critical business operations.

As cybersecurity threats grow in number and complexity, securing any business network requires a unique combination of threat intelligence, global network visibility, a broad portfolio of security services, and comprehensive 24/7 customer support to efficiently and effectively manage risks to network and data assets.

PROTECTING WHAT IS MOST IMPORTANT TO YOU

The Web has opened the door to infinite business opportunities for both your business and cybercriminals. Today, the Web is critical for businesses, with companies doing some or all of their business online, with websites and numerous applications online or stored in the cloud ... all accessed via the Web. These applications are used on a daily basis and critical to business operations for employees, customers, partners and suppliers. However, with each Web connection, you introduce another potential entry point for infections and malicious infiltration. And without the proper protections, you risk your company’s reputation, data and finances.

SECURING WEB ASSETS, INTERNET TRAFFIC AND BUSINESS CRITICAL COMMUNICATIONS

The Web has become more complex and seems to change every day, with the introduction of social media, interactive webpages and the ever-growing number of collaboration and business applications used on a daily basis. All of these changes can increase the burden on your security staff and IT professionals, making it crucial to choose the right combination of protection for your company.
SYMANTEC BLOCKED 568,700 WEB ATTACKS PER DAY IN 2013 AS COMPARED TO 464,100 IN 2012.

— SYMANTEC “INTERNET SECURITY THREAT REPORT” 2014
NETWORK-BASED SECURITY
SECURITY WITH SIMPLICITY

The end of premises-based security solutions is fast approaching, as security ecosystems comprised of multiple point solutions often check the compliance box. They, in turn, create complex operating environments, require high capital investment and introduce even more vulnerabilities. With the ever-increasing volume and complexity of threats, premises-based security architectures are becoming even more challenging to manage (monitor, update etc.). And as mobility, BYOD trends and cloud adoption take over, your IT/security staff must change the way they think about protecting your systems and data.

Migrating to a network-based security infrastructure allows for multi-tiered security, providing protection against today’s sophisticated attacks with simplified management, limited operational costs and capital investment. Don’t face the growing struggle alone – the move to an outsourced model allows you to maintain control while taking advantage of 24/7 monitoring and mitigation via a global security operations center (SOC), staffed with certified security specialists and backed by advanced threat intelligence. Maintain the visibility and control your business desires and ease the burden of managing it all yourself with the predictive protection necessary in today’s threat environment.

Level 3 Network-Based Security Platform:
- Built on a global fiber network
- Global platform able to help mitigate both network and Internet security threats
- Monitored by a state-of-the-art Security Operations Center (SOC) backed by intelligence from Level 3 Threat Research Labs
- User-friendly security analytics tool with real-time reporting capabilities

Level 3 Global Security Operations Center:
Every minute of every day, Level 3’s Global Security Operations Center (SOC) monitors and mitigates:
- 1,000 command and control servers
- Over 1 million malicious packets
- Over 1.7 million infected machines
- Over 36 million Netflow sessions per day

THANKS TO THE SOPHISTICATION AND SIZE OF OUR GLOBAL NETWORK, LEVEL 3 HAS ACCESS TO COMPREHENSIVE NETWORK SECURITY THREAT DATA.
Network-based Security

Multi-tiered Network-based Security

The Level 3 Communications network-based security portfolio provides enterprises with end-to-end, multi-layered Internet and content threat protection, helping to insulate your infrastructure and data from malicious attacks.

These network-based security services enable you to mitigate against all known forms of sophisticated distributed denial of service (DDoS) and application layer attacks, protect Web content, filter URLs and mitigate against potentially crippling virus attacks while also blocking spam.

Our user-friendly management portal, with detailed real-time security reporting tools, alerting and analytics, provides unparalleled visibility into attack traffic, ensuring better availability and business continuity.

Customer Benefits:

- Network-based deployment for faster implementation, reduced operating costs and no large capital outlay
- “Always-on” protection with access to security experts and best practices
- Proactive cyberthreat identification and management to stay ahead of evolving threats
- Safeguards network and data from Internet/Web- and email-related threats
- Ensures availability and uptime of network/Internet connections and assets (applications, Website, etc.) to help maintain business continuity.

Key Features:

- Secure Internet gateways through globally distributed infrastructure for improved latency, performance and simplified management
- Mitigate massive, sophisticated, DDoS attacks
- Leverage our email and web solutions. Block spam and prevent unwanted files carrying viruses from entering or leaving your network
- Utilize data loss prevention (DLP) and encryption capabilities for managing the flow of content within and outside your organization and securing content from prying eyes
- Gain extensive visibility into security threats; access detailed, real-time reporting and analytics

Our dedicated SOC monitors the health and availability of any security appliance deployed on your premises and within our global network on a 24 x 7 basis.
Detect and Mitigate Sophisticated Denial of Service Attacks

Level 3℠ DDoS Mitigation service offers enterprise customers cost-effective mitigation against network layer and application layer attacks. Protect your website, Web-enabled applications or your entire network against DDoS threats that can prevent employees, customers, partners and suppliers from doing business with you. Suitable for enterprises of all sizes, from enhanced network routing, rate limiting and filtering paired with an advanced mitigation (scrubbing) service that can either be deployed ‘on-demand’ or ‘always-on’, our portfolio of DDoS mitigation options provide you the flexibility to choose the most relevant and cost-effective protection model for your needs, backed by well-defined time-to-mitigate SLAs. DDoS attacks can be some of the most menacing, crippling websites and networks and shutting down online services and applications – costing your business thousands, even millions, of dollars. These types of attacks are an intimidating and costly threat to the integrity of your IP Network, applications and business.

MITIGATE ATTACKS WITH ADVANCED NETWORK FILTERING AND ROUTING

The most basic DDoS attack service, network protection, provides permanent safeguards protecting your business against volumetric attacks. Our SOC staff uses a combination of network routing and filtering techniques to stop attacks in their tracks, diverting malicious traffic away from your infrastructure.

- Null routes and permanent ACLS (50 lines or less)
- Rate limiters and upstream firewall filters
- 24/7 service provided by Level 3 Security Operation Center (SOC) and Level 3 security professionals

LEVEL 3’S GLOBAL MITIGATION NETWORK HAS A TOTAL OF 4.5 TBPS OF ATTACK INGESTION CAPACITY AND IS SUPPORTED OUT OF SEVEN REGIONAL SCRUBBING CENTERS
NEARLY 40% OF SURVEYED BUSINESSES REPORTED BEING ATTACKED FOR A DAY OR MORE WITH MORE THAN 40% OF SURVEYED BUSINESSES ESTIMATING DDOS LOSSES AT OVER $1 MILLION PER DAY.

—NEUSTAR “2014 – THE DANGER DEEPENS: NEUSTAR’S ANNUAL DDOS ATTACKS AND IMPACT REPORT”
MITIGATE ATTACKS USING PROXY AND GRE SOLUTIONS

Easy to provision and cost effective, the proxy solution is the fastest means to deploy advanced DDoS mitigation. When under or threatened by an attack, you can protect your business through a simple DNS change that redirects Internet traffic to our global mitigation network for cleansing through our network-based scrubbing center(s).

- Rapid mitigation against HTTP- or HTTPS-based Web attacks
- Provides the first layer of defense when under DDoS attack
- Easily protect individual customer domains effectively with minimal changes

A GRE solution, on the other hand, provides effective protection against network attacks for larger networks. DDoS mitigation may also be implemented in an ‘Always-On’ or ‘On Demand’ mode through the use of the generic route encapsulation (GRE) protocol. This involves the creation of a virtual wire between your network and our global mitigation network.

- Protect against DDoS attacks on multiple service types and protocols, not just HTTP and HTTPS, with volumetric and application layer attack mitigation (layers 3-7)
- Full IP address protection

MITIGATE ATTACKS USING DIRECT SOLUTIONS

The Level 3 DDoS Mitigation solution provides protection for customers with high-bandwidth requirements. This may also be implemented as ‘Always On’ or ‘On Demand’ through direct physical connections from the customer network to the Level 3 global DDoS mitigation network. It is ideal for complex, distributed customer networks running multiple applications in data center environments and if you:

- Are running existing Level 3® MPLS/IP VPN services at protected locations
- Have applications which are sensitive to latency and jitter and require a predictable underlying network
- Desire a high bandwidth “clean-pipe” connection to our global mitigation network.

Whether implementing DDoS mitigation through proxy, GRE or direct solutions, Level 3 DDoS Mitigation provides protection against all forms of DDoS traffic. These services help ensure genuine traffic and users remain unaffected during DDoS attacks, thereby ensuring your internet connection(s), hosting environments and applications remain up and running for better site availability and business continuity.

In today’s threat environment, attacks are evolving in form, complexity, volume, timing, and, more often than not, they will hit your organization from multiple angles at multiple layers. It is essential to have a layered security infrastructure with multiple safeguards for an in-depth defense solution. DDoS mitigation should be looked at as an enhancement or strengthening of your firewall and intrusion detection/prevention services, as there is a major distinction between firewall, intrusion detection/prevention solutions and DDoS mitigation. While firewalls can protect against attacks at Layer 3, they are not sufficient to protect your network from most DDoS attacks. With attackers often hitting with two-pronged attacks at both the network and application layers, it is critical for you to have a complete solution to ensure effective protection against Layer 7 application attacks.
MORE THAN 70 PERCENT OF AN AVERAGE ORGANIZATION’S TOTAL EMAIL VOLUME IS SPAM, 10 PERCENT OF SPAM MESSAGED ARE MALICIOUS AND 7 PERCENT OF THOSE CONTAIN LINKS TO MALICIOUS WEBSITES.

-MCAFEE, JAVELIN STRATEGY & RESEARCH/NOVEMBER 2012 OSTERMAN RESEARCH SURVEY ON EMAIL, WEB AND SOCIAL MEDIA SECURITY
Level 3 MSS Cloud: Secure Internet Gateways

Our network-based service consists of a completely managed, network-based firewall that can be coupled with other functions, such as intrusion detection and prevention, Web content security, URL filtering, anti-virus protection and spam blocking. The solution provides unprecedented visibility and flexibility to cost-effectively mitigate threats that could otherwise significantly compromise your business.

Layer one or more of these services with our Managed Firewall Service:

- **Intrusion Detection and Prevention** – Examine the payload of traffic that is allowed to pass your firewall to help ensure there are no hidden attacks and block direct compromise of your network infrastructure.

- **Web Content** – Create, manage and monitor content filtering policies in order to block access to Websites based on categories. Administer policy overrides based on user, group or source IP address.

- **URL Filtering** – Control your Internet access costs, boost efficiency and protect against malware. Leverage cloud- and site-based services to facilitate specific permission or denial of URLs.

- **Anti-virus/Anti-spam Service** – Block or tag unwanted email and prevent unwanted files carrying viruses from entering your network.
Content Security – Email and Web Protection
The proliferation of spam means more malware, fraud, email attacks and other threats that need to be identified and blocked. It is not sufficient for businesses to simply secure their connections to applications and the Internet. With the growth of Web-born malware and email threats (phishing, spam, social engineering, malware payloads, etc.), it is critical for you to have security for these avenues of attack. This cannot be left up to the end users knowing when to delete an email or not click a malicious link, because they don’t know. In today’s business environment, organizations are increasingly reliant on the Web and email for communications and everyday business – and attackers have taken notice.

It is too common for users to open unsolicited emails or attachments, click on malicious links, or unknowingly visit malicious sites or content on the Web. Your organization needs to make sure that malicious sites/Web content, emails and their attachments are filtered out or blocked. Level 3 provides advanced protection against Web-born malware with Web content and URL filtering to ensure safe and productive Web usage, which is complemented by our anti-virus and anti-spam filtering capabilities for safe and secure email communications. Not only will these services limit the amount of mail in your employees’ mailboxes, cutting down on spam and increasing productivity, they will help filter out files/attachments carrying viruses. In this day and age, you cannot simply rely on “vigilant” or “knowledgeable” employees knowing what to do with their email and while working on the Web.

EXPERT SERVICE MANAGEMENT MONITORING, THREAT ANALYSIS AND MITIGATION
Level 3’s state-of-the-art Security Operations Center (SOC) leverages our global IP and CDN networks to gain visibility into potential cyber threats. Two mirrored sites enable concurrent, site-level business continuity and disaster recovery.

GLOBAL SECURITY OPERATIONS CENTER
RELY ON THE LEVEL 3 SOC
Proactive detection and mitigation of security threats
Reactive response to security issues including physical and logical alarms, attacks, suspicious or other abnormal network activities
24 x 7 monitoring and support provides proactive vigilance against internal and external threats
Ensures information confidentiality, integrity and availability
OUR DEDICATED SOC

MONITORS THE HEALTH AND AVAILABILITY OF ANY SECURITY APPLIANCES DEPLOYED ON YOUR PREMISES OR WITHIN OUR NETWORK ON A 24/7 BASIS. EVENT LOGS AND ALERTS GENERATED BY OUR SECURITY ASSETS ARE CORRELATED, CLASSIFIED AND ANALYZED USING OUR CUSTOMIZED SECURITY INCIDENT AND EVENT MONITORING (SIEM) PLATFORM. OUR SKILLED SECURITY ANALYSTS INTERPRET THIS INFORMATION AND WILL WORK WITH YOUR IT SECURITY PERSONNEL TO MANAGE ANY POTENTIAL NETWORK THREATS. WE WILL PROACTIVELY INVESTIGATE INCIDENTS AND ANALYZE THE LIKELIHOOD AND IMPACT OF THREATS ON YOUR CRITICAL NETWORK ASSETS, WHILE RESPONDING QUICKLY AND APPROPRIATELY.
MYLEVEL3℠ CUSTOMER PORTAL AND SECURITY ANALYTICS TOOL

In addition to the support of our security operations team, your organization requires real-time, anytime access to your data. The My Level 3℠ Portal and security analytics tool provides the reporting you need to manage your specific security implementation.

Complete view of security platform for policies, configuration rules, consumption data and security elements

A consolidated tool providing a single point of reference to monitor cyber security events in real-time, and examine clean/attack traffic, user activity, web and email reports, etc.

Administer security policies and configurations online through tickets to the SOC

Manipulate and filter data to create custom downloadable reports

Real-time reporting on device health and availability of your security appliances managed by Level 3
Support Continuity of Operations. With the sophistication and complexity of attacks, enterprises typically do not have the internal resources or knowledge base to manage risk to their network. Level 3 has the people and analytics tools in place to see threats and attacks across multiple network service portfolios.

Manage Risk to Your Brand and Intellectual Property. You are tasked with protecting your organization’s proprietary data and maintaining your brand integrity. The complexity, volume and nature of threats require coordinated and knowledgeable personnel on duty every minute of every day. Level 3’s Security Operations Center (SOC) provides 24/7 monitoring and threat analysis.

Manage Operational Complexity. Cyberthreats are constantly changing in form, volume, timing and points of origin. Most organizations do not have the budget to hire experts to manage these dynamics, and also focus on their core business. Integrated security and network capabilities allow Level 3 to stay on top of and coordinate events across global infrastructures.
Level 3 Communications, Inc. (NYSE: LVLT) is a Fortune 500 company that provides local, national and global communications services to enterprise, government and carrier customers. Level 3’s comprehensive portfolio of secure, managed solutions includes fiber and infrastructure solutions; IP-based voice and data communications; wide-area Ethernet services; video and content distribution; and data center and cloud-based solutions. Level 3 serves customers in more than 500 markets in over 60 countries across a global services platform anchored by owned fiber networks on three continents and connected by extensive undersea facilities. For more information, please visit www.level3.com or get to know us on Twitter, Facebook and LinkedIn.
We build, operate and take end-to-end responsibility for network solutions that connect you to the world. We put customers first and take ownership of reliability and security across our broad portfolio.