Your network is your business lifeline. Protect it.

LEVEL 3® ADAPTIVE NETWORK SECURITY
CHAPTER 01
WHY ACT NOW?

CHAPTER 02
THE BENEFITS OF NETWORK-BASED SECURITY

CHAPTER 03
GET TO KNOW LEVEL 3 ADAPTIVE NETWORK SECURITY

CHAPTER 04
WHY LEVEL 3?

CHAPTER 05
SAFEGUARD YOUR NETWORK

NAVIGATION TIP: The plus signs and arrows in this document are clickable and lead to more information.
WHY ACT NOW?

LEVEL 3® ADAPTIVE NETWORK SECURITY

Internet connectivity has never been more important to your enterprise. It makes your workforce mobile, facilitates global collaboration and allows you to increase the agility of your business.

But expanded internet connectivity also creates new security concerns. In hybrid public-private network environments, your perimeter has changed. Your network can be attacked from anywhere. An innocent-seeming email or errant click on a malicious website can take down your enterprise. And increased reliance on accessibility means increased risk to valuable data.

72% Increase in new mobile malware samples between Q3 and Q4 2015.¹

26% Increase in new ransomware samples between Q3 and Q4 2015, more than double the total from the same period in the prior year.²

MSS 2.0 allows security professionals to leverage the network to improve cybersecurity and appropriately respond to attacks and incursions that MSS 1.0 misses.

Traditional Premises-Based Solutions (MSS 1.0)

Enterprise Security Gateway (MSS 2.0)

Premises-based security puts the pressure on internal IT staff to manage security across locations.

Adaptive Network Security solutions are built into the network, lowering cap-ex costs without sacrificing performance.

<table>
<thead>
<tr>
<th>USER DEVICE</th>
<th>Company-provided</th>
<th>BYOD / mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>MANAGEMENT</td>
<td>In-sourcing only</td>
<td>Allows for outsourcing</td>
</tr>
<tr>
<td>DELIVERY</td>
<td>Dedicated premises-based devices</td>
<td>Network-based shared infrastructure</td>
</tr>
<tr>
<td>DETECTION</td>
<td>Reactive through signature-based analysis</td>
<td>Predictive through behavioral data analysis</td>
</tr>
<tr>
<td>ALERT</td>
<td>Event-based Security Operations Center (SOC) / security information and event management support</td>
<td>Predictive analysis and alerting</td>
</tr>
</tbody>
</table>

Level 3 has an expansive view of the threat landscape and highly trained security professionals who track and mitigate the threat of malicious activity.

LEVEL 3® ADAPTIVE NETWORK SECURITY

Internet connectivity has never been more important to your enterprise. It makes your workforce mobile, facilitates global collaboration and allows you to increase the agility of your business.

But expanded internet connectivity also creates new security concerns. In hybrid public-private network environments, your perimeter has changed. Your network can be attacked from anywhere. An innocent-seeming email or errant click on a malicious website can take down your enterprise. And increased reliance on accessibility means increased risk to valuable data.

72% Increase in new mobile malware samples between Q3 and Q4 2015.¹

26% Increase in new ransomware samples between Q3 and Q4 2015, more than double the total from the same period in the prior year.²

MSS 2.0 allows security professionals to leverage the network to improve cybersecurity and appropriately respond to attacks and incursions that MSS 1.0 misses.

Traditional Premises-Based Solutions (MSS 1.0)

Enterprise Security Gateway (MSS 2.0)

Premises-based security puts the pressure on internal IT staff to manage security across locations.

Adaptive Network Security solutions are built into the network, lowering cap-ex costs without sacrificing performance.

<table>
<thead>
<tr>
<th>USER DEVICE</th>
<th>Company-provided</th>
<th>BYOD / mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>MANAGEMENT</td>
<td>In-sourcing only</td>
<td>Allows for outsourcing</td>
</tr>
<tr>
<td>DELIVERY</td>
<td>Dedicated premises-based devices</td>
<td>Network-based shared infrastructure</td>
</tr>
<tr>
<td>DETECTION</td>
<td>Reactive through signature-based analysis</td>
<td>Predictive through behavioral data analysis</td>
</tr>
<tr>
<td>ALERT</td>
<td>Event-based Security Operations Center (SOC) / security information and event management support</td>
<td>Predictive analysis and alerting</td>
</tr>
</tbody>
</table>

Level 3 has an expansive view of the threat landscape and highly trained security professionals who track and mitigate the threat of malicious activity.
THE RISKS ARE ON THE RISE

GROWING THREATS REQUIRE BETTER ANSWERS

As the threat and costs of a security breach continue to grow, the scarcity of in-house security expertise compounds the challenges of defending your data. Many companies are struggling to keep up, and initiatives to upgrade their security posture often outpace staffing capabilities. Network-based security outsourcing reduces capital expenses and adds external expertise to your security team.

Your network can be accessed from everywhere. To protect your business and your data, you need a security solution that can help proactively stop threats from anywhere. You need Adaptive Network Security.

$3.79 MILLION
The average total cost of a data breach in 2015.

21%
During the past two years, security spending as a percentage of the total IT budget remained strong at about 21% across most industry sectors.
THE BENEFITS OF NETWORK-BASED SECURITY

NETWORK-BASED SECURITY IS THE FOUNDATION

Traditional point security solutions have had their day. Reactive and isolated, point solutions are poorly suited for the complexities of modern business environments and the evolving nature of threats. They’re labor intensive, expensive and provide little visibility into the overall fitness of your security posture.

Proactive, network-based security replaces coverage gaps and complex management burdens of point solutions with a holistic, multilayered security posture. By integrating the latest technologies into the network, security management operations can be simplified and capital investments reduced.

To perform and protect at its best, network-based security should act as the foundation to a suite of managed services. Level 3 Adaptive Network Security augments our robust network-based security options by providing an array of managed security features. This powerful combination is a comprehensive approach and represents the next generation of network security.

DETECT
Our global Security Operations Centers in North America, Latin America and Europe vigilantly monitor our network and systems 24/7 for physical and virtual malicious activity.

PREDICT
We have a broad view of the threat landscape and the ability to track potential bad actors across the internet.

SECURE
Adaptive Network Security provides global protection closer to the edge, near the point of attack.

ALERT
Adaptive Network Security alerts you to threats and helps you decide what actions to take next.

THE BENEFITS OF
NETWORK-BASED
SECURITY
THE BENEFITS OF NETWORK-BASED SECURITY

We predict malicious activity through analytics that unlock insights into global threats.

Our unique perspective and vast global network gives the security experts in the Level 3 Threat Research Labs both a broad view of the threat landscape and the ability to track potential bad actors across the internet. Bad actor profiles are defined based on “big data” behavioral analytics, threat intelligence research and third-party correlation.
THE BENEFITS OF NETWORK-BASED SECURITY

NETWORK-BASED SECURITY

PREDICT  DETECT  ALERT  SECURE

We use predictive insights to help detect potential issues and expose attacks before they occur.

The Level 3 global network acts as a sensor for anomalous traffic. Armed with rich threat intelligence, experts in our global Security Operations Centers vigilantly monitor our network and systems 24/7 for indicators of physical and virtual malicious activity. By leveraging insight gained through our deep visibility across multiple network layers, we are able to shut down attacks at the source in many cases, before they damage our customers’ data or infrastructure.

The benefits of network-based security

Traditional point security solutions have had their day. Reactive and isolated, point solutions are poorly suited for the complexities of modern business environments and the evolving nature of threats. They’re labor intensive, expensive and provide little visibility into the overall fitness of your security posture.

Proactive, network-based security replaces coverage gaps and complex management burdens of point solutions with a holistic, multilayered security posture. By integrating the latest technologies into the network, security management operations can be simplified and capital investments reduced.

To perform and protect at its best, network-based security should act as the foundation to a suite of managed services. Level 3 Adaptive Network Security augments our robust network-based security options by providing an array of managed security features. This powerful combination is a comprehensive approach and represents the next generation of network security.
THE BENEFITS OF NETWORK-BASED SECURITY

NETWORK-BASED SECURITY

PREDICT  DETECT  ALERT  SECURE

We alert you to threats and help you know what actions you should take next.

Depending on the type and severity of attack, our customers may receive a call from one of our global Security Operations Centers or they may receive auto-alerts, firewall updates or auto-mitigation when threats arise. Customers may also call into our Security Operations Center to initiate security countermeasures. Our customer portal, with two-factor user authentication, provides secure access to alerts, mitigation efforts, and reports.

Level 3 Adaptive Network Security augments our robust network-based security options by providing an array of managed security features. This powerful combination is a comprehensive approach and represents the next generation of network security.
**THE BENEFITS OF NETWORK-BASED SECURITY**

**NETWORK-BASED SECURITY**

**PREDICT  DETECT  ALERT  SECURE**

*We secure the network to ensure that your critical information and infrastructure is protected.*

Network-based security solutions provide protection closer to the edge, near the point of attack. DDoS mitigation, network-based managed firewall, unified threat management (UTM), email and web protection, and real-time security reporting can all be managed efficiently and effectively right in the network.

Your network is protected 24/7 by our global Security Operations Centers, which continuously monitor the threat landscape and are “on call” whenever your team needs additional support. Our security countermeasures can be enacted on your behalf depending upon global threat intelligence, all based on mutually agreed-upon scenarios.
ADAPTIVE NETWORK SECURITY BRINGS NEW LEVELS OF PROTECTION

Level 3 Adaptive Network Security provides a stronger and more flexible security posture than was possible under traditional point solution schemes. This flexibility extends to all organizations—whether they are current Level 3 network customers those leveraging third-party ISPs—allowing them to take advantage of these technologies and services, on-net or off.

At its heart, Adaptive Network Security is a next-generation firewall built on the proven foundation of networked-based security. Network-based security is integral to cloud security, the emerging global model. By routing all network traffic through an inherently secure gateway, the solution delivers highly controlled connections that can help minimize exposure to new, unexpected and unnecessary risks.

Adaptive Network Security features can be customized and are available individually to support your unique network and security posture.

PREVENTIVE MULTI-LAYERED SECURITY LOGGING, ANALYTICS AND INTELLIGENCE
Level 3® Adaptive Network Security offers preventive, multi-layered security solutions, including:

- **Next-Generation Managed Firewall**
- **Intrusion Detection and Prevention**
- **Web Content and URL Filtering**
- **Secure Access**
- **Data Loss Protection**
- **Application Awareness and Control**
- **Malware Sandboxing**

Logging, analytics and (threat) intelligence are tools available across all of the features.
GET TO KNOW

NEXT-GENERATION MANAGED FIREWALL

Level 3℠ Managed Firewall helps businesses easily manage complex security environments across the continuously evolving threat landscape. We monitor, block and report on attempts to compromise your network. In the process, we supply the detailed information you need to track threats more effectively and better protect your organization against whatever tomorrow brings.

Along with providing increased visibility, Level 3 can tailor your firewall to meet the distinct needs of your business, providing or restricting access to help reduce human error while allowing for necessary connectivity. Easily access online reporting of threats and control of firewalls through our portal interface.

Logging, analytics and (threat) intelligence are tools available across all of the features.
GET TO KNOW

INTRUSION DETECTION AND PREVENTION

The devices you use, your location, your infrastructure and even your company culture can influence security risks. Level 3’s Intrusion Detection and Prevention services are specifically tuned to your organization — and your network — to effectively identify attacks, isolate intruders and mitigate false positives.

Intrusion Detection adds a layer of security to firewall protection by examining payload traffic to help eliminate hidden attacks. At the same time, we give you the insight you need to understand the threats to your network for continuous improvement and a proactive defense. Our portal interface provides reporting on intrusions detected and stopped.

Logging, analytics and (threat) intelligence are tools available across all of the features.
GET TO KNOW

WEB CONTENT / URL FILTERING

Malware, ransomware and spyware are attacking your network. At the same time, some threats inadvertently find their way into your network. An innocent-appearing email or accidental visit to a malicious website can place your infrastructure at risk. One bad click can introduce a virus that threatens your entire enterprise.

Level 3 knows where the malicious code is hiding. We monitor how internet resources are used, track bad URLs and websites, and inspect downloaded web content before it can infect your systems.

Level 3SM Web Content Filtering is integrated with an Active Directory server for granular access and reporting to help ensure that the right people have the access they need, without compromising your business.

Logging, analytics and (threat) intelligence are tools available across all of the features.
GET TO KNOW
SECURE ACCESS

Your employees, customers, vendors and partners want access to your network from anywhere, on any device, so keeping your connections secure has never been more important.

Managing and securing and mobile access can be overwhelming, but it doesn’t have to be. Make it simple, with Level 3.

Level 3SM Secure Access can give your users an easy, safe path to your critical data, wherever it lives. Our security experts assess your remote and mobile needs, before designing tailor-made solutions that extend the security policies of your core network to every end user — without running up costs.
GET TO KNOW

DATA LOSS PROTECTION

Your data is one of your most valuable assets — and it has the greatest potential for misuse. When the exchange and movement of intellectual property, confidential information, trade secrets and other sensitive data are crucial to your business, how do you make sure this information goes only where you want it to?

Adaptive Network Security can help. It monitors and tracks the movement of your most sensitive data and alerts you to intentional and accidental attempts to distribute it outside of your organization. With our granular, file-based approach, you can detect, track and block unauthorized attempts to move critical information.
GET TO KNOW

APPLICATION AWARENESS AND CONTROL

Malware is often distributed through popular web-based applications such as social media. Application Awareness can identify, report on and enforce application compliance across your organization, alerting you to risky behavior and inappropriate usage. Designed for flexibility, Application Awareness enables granular, policy-based control over application availability, with access customizable by user.
GET TO KNOW
MALWARE SANDBOXING

Malware and ransomware are coming for your employees, systems and network. Adaptive Network Security malware sandboxing can help stop them. We scan network traffic for malicious code and confine suspicious payloads in isolated sandbox environments.

Once we know they’re safe, benign payloads are released. And if a suspect payload is confirmed as malicious, a unique threat signature is created and pushed out across the network to help detect other dangers and mitigate the chance of future attacks.

Logging, analytics and (threat) intelligence are tools available across all of the features.
WHY LEVEL 3?

THE LEVEL 3 DIFFERENCE

Level 3 understands the threat landscape — and its dangers — and has developed a deep understanding of the challenges associated with providing secure connectivity.

Our vantage point and global footprint allow us to track large volumes of internet traffic for malicious activity, helping our Threat Research team understand where threats originate. With this insight, we are able to take swift action to mitigate botnet behavior, distributed denial-of-service attack patterns and other attack types. Level 3\textsuperscript{TM} Threat Research Labs help protect your network, systems and data.

Level 3 has deployed Security Operations Centers (SOC) in strategic global locations and staffs these SOCs with highly experienced cybersecurity experts who continuously monitor the global threat landscape. Our SOCs respond to physical and logical alarms, attacks, and suspicious or abnormal network activity, as well as assist with your security inquiries.

LEVEL 3 SOCs PROTECT MORE THAN 200,000 ROUTE MILES OF FIBER GLOBALLY, 120,000 NETWORK ELEMENTS AND 20,000 ENTERPRISE CUSTOMERS.

REAL-WORLD SUCCESS

LEVEL 3 THREAT RESEARCH LABS TRACK DOWN LINUX MINT HACK

- 1.3 BILLION
  Number of security threats Level 3 monitors per day\textsuperscript{4}

- 3 MILLION
  Number of compromised computers Level 3 tracks each day\textsuperscript{7}
WHY
LEVEL 3?

THE LEVEL 3 DIFFERENCE

Level 3 understands the threat landscape — and its dangers — and has developed a deep understanding of the challenges of associated with providing secure connectivity.

Our vantage point and global footprint allow us to track large volumes of Internet traffic for malicious activity, helping our Threat Research team understand where threats originate. With this insight, we are able to take swift action to mitigate botnet behavior, distributed denial-of-service attack patterns and other attack types. Level 3’s threat research helps protect your network, systems and data.

Level 3 has deployed Security Operations Centers (SOC) in strategic global locations and staffs these SOCs with highly experienced cybersecurity experts who continuously monitor the global threat landscape. Our SOCs respond to physical and logical alarms, attacks, and suspicious or abnormal network activity, as well as assist with your security inquiries.

LEVEL 3 THREAT RESEARCH LABS TRACK DOWN LINUX MINT HACK

When Linux Mint, one of the most popular Linux desktop distributions, had its installation image accessed through a backdoor, links on Linux Mint’s homepage were replaced by links to a malicious site. Linux Mint was quick to offer transparency about the attack, but it didn’t say when exactly traffic began being redirected to the malicious sites. For this kind of attack, an accurate timeline is crucial to understanding and evaluating the risks. Data collected by Level 3 Threat Research Labs confirmed that impact was worse than what had been reported by other sources to date.

Number of security threats Level 3 monitors per day

1.3 BILLION

Number of compromised computers Level 3 tracks each day

3 MILLION

REAL-WORLD SUCCESS
SAFEGUARD YOUR NETWORK

TAKE ACTION TO PROTECT YOUR BUSINESS

Greater security than traditional point security solutions. Multilayered protection. Less complexity. Simpler management.

It’s time for Level 3 Adaptive Network Security.

Getting started is easy. Our security solutions architects are ready to assess your current security infrastructure and explore how we can help keep your organization secure within the ever-evolving global threat landscape.

If you’re currently planning a network expansion, this may be the perfect time to improve your security posture. Level 3 can implement Adaptive Network Security on the expanded network area only, so you can experience the benefits firsthand, before committing to a larger footprint.

Learn more about Level 3 Adaptive Network Security services and the many ways that Level 3 can help lock down your network, protect your employees and secure your digital assets.

TAKE CONTROL OF YOUR NETWORK SECURITY. OWN YOUR DEFENSE.

WATCH THE ADAPTIVE NETWORK SECURITY VIDEO.

Level 3 connects business locations, data centers and cloud service providers through a global network of more than 200,000 route miles of fiber connecting 60+ countries.