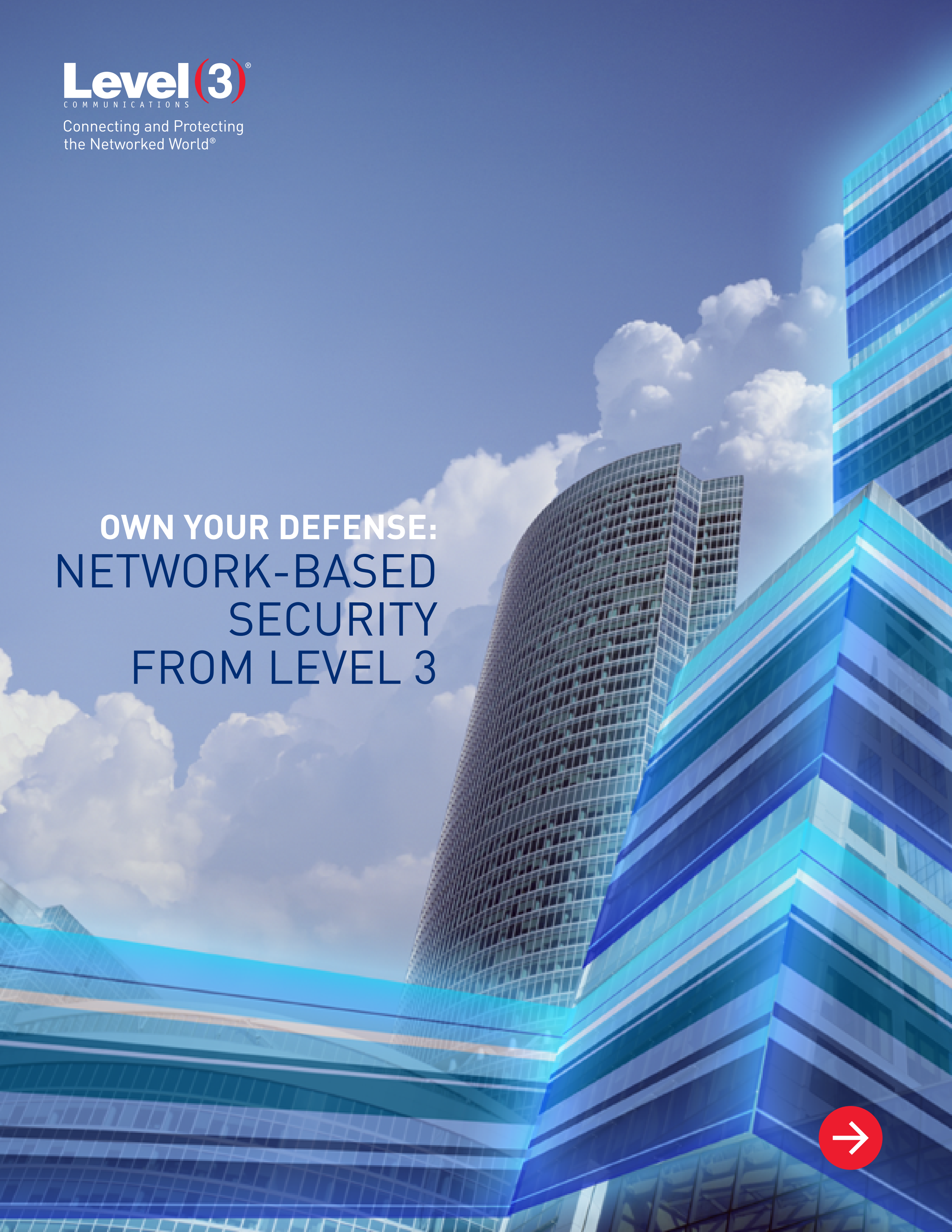


Level(3) COMMUNICATIONS

Connecting and Protecting
the Networked World®

OWN YOUR DEFENSE:
NETWORK-BASED SECURITY FROM LEVEL 3

TABLE OF CONTENTS

FACE THE FUTURE **WITH CONFIDENCE**

It's ironic; many of the same things that drive business forward today are often the primary points of entry or vectors of attack that can damage your organization.

Mobile workers accessing networks through an array of devices can increase productivity and collaboration—but create new challenges for maintaining firewalls. New channels and platforms for deploying applications and engaging with customers can improve brand loyalty—but open new points of vulnerability. Nearly seamless anytime, anywhere access to information can help drive sales on a 24-hour cycle—but requires eternal vigilance.

WE HAVE A DIFFERENT PERSPECTIVE ON SECURITY +

With the right defense, you can move ahead with confidence. It starts with network-based security from Level 3.

FACE THE FUTURE

CONFI

It’s ironic; many of the same things that drive

ften the primary

attack that can

rough an array of

collaboration—but

firewalls. New

applications and

brand loyalty—but

ly seamless anytime,

elp drive sales on a

gilance.

CLOSE ✕

WE HAVE A DIFFERENT PERSPECTIVE ON SECURITY

Threats to your organization can come from anywhere. That’s why it’s essential to have security intelligence based on global visibility across multiple network layers and service portfolios. Level 3 provides this perspective, identifying and defending against threats, including those that may have gone undetected by traditional patchwork security solutions. And because we offer network-based security, the porous nature of point solutions is eliminated.

WE HAVE A DIFFERENT PERSPECTIVE ON SECURITY ⊕

With the right defense, you can move ahead with confidence. It starts with network-based security from Level 3.

NAVIGATING THE THREAT LANDSCAPE

Every new connection among your systems, employees, partners and customers is a potential point of vulnerability.

PRIMARY RISKS ACROSS TODAY’S THREAT LANDSCAPE:

- **Network and application layer attacks, such as distributed denial of service (DDoS)**
  Frequency: Very common
- **Social Engineering—Phishing**
  Frequency: Very common
- **Various strains of malware**
  Frequency: Increasing every year
- **Zero-day attacks**
  Frequency: Moderate, but increasing rapidly
- **Device loss or theft**
  Frequency: Very common

72% OF CYBERSECURITY EVENTS WERE TRACED TO MALICIOUS OUTSIDERS[1]

28% WERE DUE TO MALICIOUS OR ACCIDENTAL ACTIONS BY INSIDERS[2]

[1] “The Global State of Information Security Survey: 2014,” PwC, September 2013.

[2] Ibid.

NAVIGATING THE THREAT LANDSCAPE

Every new connection among your systems, employees, partners and customers is a potential point of vulnerability.

PRIMARY RISKS ACROSS TODAY'S THREAT LANDSCAPE:

Network and application layer attacks, such as distributed denial of service (DDoS)

Frequency: Very common

- Disrupts servers and network resources connected to the Internet
- Attack packages easy to find on the black market
- Often launched to distract focus from other attacks or fraudulent transactions

Social Engineering—Phishing

Frequency: Very common

Various strains of malware

Frequency: Increasing every year

Zero-day attacks

Frequency: Moderate, but increasing rapidly

Device loss or theft

Frequency: Very common

72% OF CYBERSECURITY EVENTS WERE TRACED TO MALICIOUS OUTSIDERS[1]

28% WERE DUE TO MALICIOUS OR ACCIDENTAL ACTIONS BY INSIDERS[2]

[1] "The Global State of Information Security Survey: 2014," PwC, September 2013.

[2] Ibid.

NAVIGATING THE THREAT LANDSCAPE

Every new connection among your systems, employees, partners and customers is a potential point of vulnerability.

PRIMARY RISKS ACROSS TODAY'S THREAT LANDSCAPE:

Network and application layer attacks, such as distributed denial of service (DDoS)

Frequency: Very common

Social Engineering—Phishing

Frequency: Very common

- Uses psychological manipulation to get people to perform certain actions or divulge confidential information, such as login credentials or other personally identifying information.
- Difficult to detect, as the email source often appears legitimate

Various strains of malware

Frequency: Increasing every year

Zero-day attacks

Frequency: Moderate, but increasing rapidly

Device loss or theft

Frequency: Very common

72% OF CYBERSECURITY EVENTS WERE TRACED TO MALICIOUS OUTSIDERS[1]

28% WERE DUE TO MALICIOUS OR ACCIDENTAL ACTIONS BY INSIDERS[2]

[1] "The Global State of Information Security Survey: 2014," PwC, September 2013.

[2] Ibid.

NAVIGATING THE THREAT LANDSCAPE

Every new connection among your systems, employees, partners and customers is a potential point of vulnerability.

PRIMARY RISKS ACROSS TODAY'S THREAT LANDSCAPE:

Network and application layer attacks, such as distributed denial of service (DDoS)

Frequency: Very common

Social Engineering—Phishing

Frequency: Very common

Various strains of malware

Frequency: Increasing every year

- **Spyware**
  Software that threatens privacy due to malicious redirecting (hijacking) of users to servers that secretly collect users' data
- **Ransomware**
  Malicious code that holds victims' data hostage until a "ransom" fee is paid
- **Viruses, Trojans and worms**
  Various types of malicious code that infiltrate IT systems, consume resources, inflict damage to critical systems, or steal or destroy data

Zero-day attacks

Frequency: Moderate, but increasing rapidly

Device loss or theft

Frequency: Very common

72% OF CYBERSECURITY EVENTS WERE TRACED TO MALICIOUS OUTSIDERS[1]

28% WERE DUE TO MALICIOUS OR ACCIDENTAL ACTIONS BY INSIDERS[2]

[1] "The Global State of Information Security Survey: 2014," PwC, September 2013.

[2] Ibid.

NAVIGATING THE THREAT LANDSCAPE

Every new connection among your systems, employees, partners and customers is a potential point of vulnerability.

PRIMARY RISKS ACROSS TODAY'S THREAT LANDSCAPE:

- **Network and application layer attacks, such as distributed denial of service (DDoS)**
  Frequency: Very common
- **Social Engineering—Phishing**
  Frequency: Very common
- **Various strains of malware**
  Frequency: Increasing every year
- **Zero-day attacks**
  Frequency: Moderate, but increasing rapidly
  - Vulnerabilities in software that are exploited by hackers before a "fix" can be developed and applied
- **Device loss or theft**
  Frequency: Very common

72% OF CYBERSECURITY EVENTS WERE TRACED TO MALICIOUS OUTSIDERS[1]

28% WERE DUE TO MALICIOUS OR ACCIDENTAL ACTIONS BY INSIDERS[2]

[1] "The Global State of Information Security Survey: 2014," PwC, September 2013.

[2] Ibid.

NAVIGATING THE THREAT LANDSCAPE

Every new connection among your systems, employees, partners and customers is a potential point of vulnerability.

PRIMARY RISKS ACROSS TODAY'S THREAT LANDSCAPE:

- **Network and application layer attacks, such as distributed denial of service (DDoS)**
  Frequency: Very common
- **Social Engineering—Phishing**
  Frequency: Very common
- **Various strains of malware**
  Frequency: Increasing every year
- **Zero-day attacks**
  Frequency: Moderate, but increasing rapidly
- **Device loss or theft**
  Frequency: Very common
  - Increasingly dangerous due to penetration of BYOD policies and the expanding mobile workforce

72% OF CYBERSECURITY EVENTS WERE TRACED TO MALICIOUS OUTSIDERS[1]

28% WERE DUE TO MALICIOUS OR ACCIDENTAL ACTIONS BY INSIDERS[2]

[1] "The Global State of Information Security Survey: 2014," PwC, September 2013.

[2] Ibid.

EXPERTS SAY IF YOU HAVEN'T YET BEEN ATTACKED **YOU WILL BE—AND SOON**

EVERY MONTH, YOU FACE

17 ATTACKS BY MALICIOUS CODES[3]

12 SUSTAINED PROBES[3]

10 INCIDENTS OF UNAUTHORIZED ACCESS[3]

[3] Ponemon Institute, 2014 Cost of a Data Breach Study

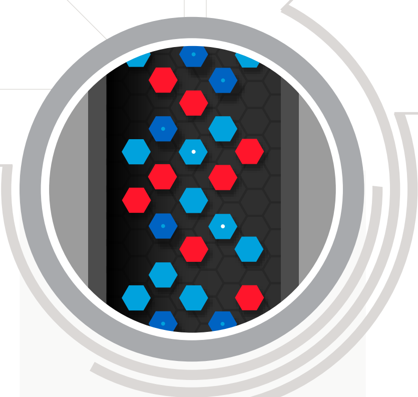
INCREASING THREATS

6.2 BILLION MALICIOUS ATTACKS ON USER COMPUTERS AND MOBILE DEVICES BLOCKED IN 2014, 1 BILLION MORE THAN IN 2013[4]

12,100 MOBILE BANKING TROJANS IDENTIFIED, 9 TIMES AS MANY AS IN 2013[4]

295,500 NEW MOBILE MALICIOUS PROGRAMS IDENTIFIED—2.8 TIMES MORE THAN IN 2013[4]

[4] Kaspersky Labs research, based on users of their security software"



EFFECT ON BUSINESS

FINANCIAL IMPACT

$6.2 BILLION AVERAGE COST OF A DATA BREACH IN 2014[5]

23% INCREASE SINCE 2013

LOST BUSINESS VALUE

$5.6 MILLION IN 2015 FOR COSTS PER INCIDENT ASSOCIATED WITH CUSTOMER TURNOVER, NEW CUSTOMER ACQUISITION, DAMAGE TO REPUTATION AND GOODWILL—NEARLY 4X GREATER THAN IN 2014

[5] Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, May 2015

OUR PERSPECTIVE ON SECURITY

The sophistication, persistence and global nature of today's complex cyber threats require a more effective defense. Our approach is rooted in the idea that we're all stronger when we work together to take on these increasingly difficult challenges.

Attackers commonly share their expertise and methods. The security community must partner as well. Collaboration will benefit everyone as we leverage our combined expertise and strategies for safeguarding data while maintaining privacy.

REAL-WORLD SUCCESS

COLLABORATING TO TAKE DOWN SSHPsychos +

Level 3 actively seeks opportunities to work with leading security organizations to strengthen the security profile of our customers and the Internet in general. That collaboration, along with our truly global reach and comprehensive vantage point as a major builder and operator of the fiber networks that connect the world, gives us the ability to see more threats as they develop–and stop them before they mature.

82% OF COMPANIES WITH HIGH-PERFORMING SECURITY PRACTICES COLLABORATE WITH OTHERS TO DEEPEN THEIR KNOWLEDGE OF SECURITY AND THREAT TRENDS.[6]

[6] PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2014, September 2013

OUR PERSPECTIVE **ON SECURITY**

e and global
er threats require
approach is
ll stronger when
hese increasingly

se and methods.
s well. Collaboration
combined expertise
le maintaining privacy.

CLOSE ✕

COLLABORATING TO TAKE DOWN SSHPsychos

During September 2014, the information security community identified an emerging persistent threat to Internet traffic. Nicknamed SSHPsychos, the new botnet demonstrated an ability to launch massive DDoS attacks Internet-wide. Level 3's Threat Research Labs and Cisco's Talos Group worked together to investigate the threat, block its traffic from the Level 3 network, and perform outreach to other network operators globally to remove it from the Internet.

REAL-WORLD SUCCESS

COLLABORATING TO TAKE DOWN SSHPsychos +

82% OF COMPANIES WITH HIGH-PERFORMING SECURITY PRACTICES COLLABORATE WITH OTHERS TO DEEPEN THEIR KNOWLEDGE OF SECURITY AND THREAT TRENDS.[6]

Level 3 actively seeks opportunities to work with leading security organizations to strengthen the security profile of our customers and the Internet in general. That collaboration, along with our truly global reach and comprehensive vantage point as a major builder and operator of the fiber networks that connect the world, gives us the ability to see more threats as they develop–and stop them before they mature.

[6] PwC, CSO magazine, CIO magazine, The Global State of Information Security® Survey 2014, September 2013

WE SEE MORE, SO WE STOP MORE

Certified security professionals operate the Level 3 Threat Research Lab and our globally dispersed Security Operations Centers (SOCs).

DEVELOPING ACTIONABLE THREAT INTELLIGENCE

REAL-WORLD SUCCESS

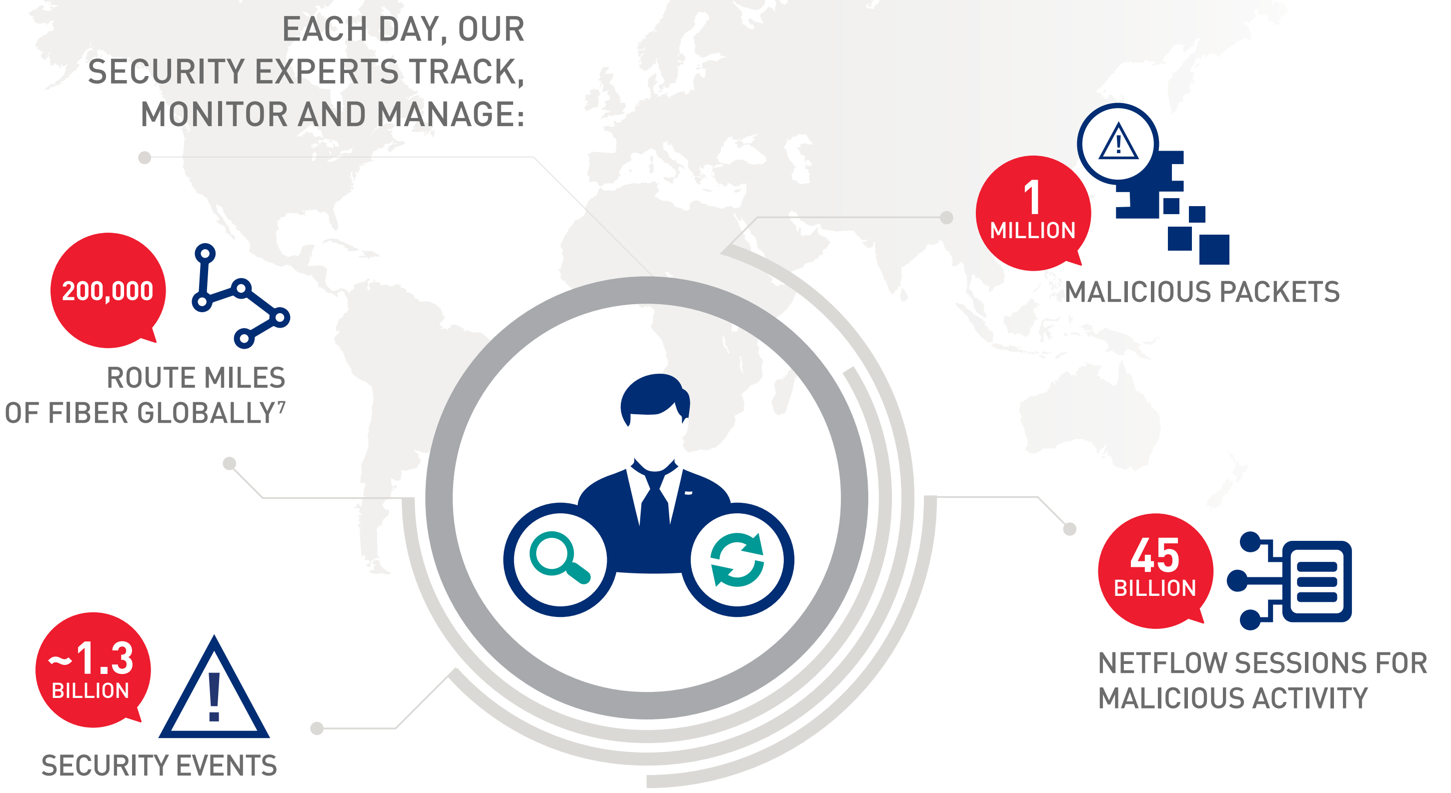
LEVEL 3 TAKES ON POSEIDON ⊕

LEVEL 3 THREAT RESEARCH LABS

Security specialists monitor communications between malicious actors and their victims, enabling us to predict risks, detect attacks and track zero day exploits.

SECURITY OPERATIONS CENTERS

Staffed 24x7 with analysts and engineers ready to efficiently respond to your security issues, our SOCs respond to physical and logical alarms, attacks, and suspicious or abnormal network activity.



EACH DAY, OUR SECURITY EXPERTS TRACK, MONITOR AND MANAGE:

200,000 ROUTE MILES OF FIBER GLOBALLY[7]

1 MILLION MALICIOUS PACKETS

~1.3 BILLION SECURITY EVENTS

45 BILLION NETFLOW SESSIONS FOR MALICIOUS ACTIVITY

[7] Level 3 internal research

WE SEE MORE, SO WE STOP MORE

Certified security professionals operate the Level 3 Threat Research Lab and our glob

CLOSE ✕

DEVELOPING ACTIONABLE THREAT INTELLIGENCE

We monitor command and control servers worldwide, along with known malware and phishing domains, giving us deep visibility into where threats originate. Every day, experts in our Threat Research Labs proactively analyze the global threat landscape, sharing that information to help defend our customers and the public Internet. We also track communications traffic, seeking abnormalities such as changes in traffic patterns, which can indicate an impending attack. Armed with this threat information, Level 3 acts to protect our customers and our network.

D
A
IN

RCH LABS

communications between
tims, enabling us to predict
k zero day exploits.

RE

LI
P

CENTERS

d engineers ready to efficiently
es, our SOCs respond to
attacks, and suspicious or
abnormal network activity.

EACH DAY, OUR SECURITY EXPERTS TRACK, MONITOR AND MANAGE:

200,000 ROUTE MILES OF FIBER GLOBALLY[7]

1 MILLION MALICIOUS PACKETS

~1.3 BILLION SECURITY EVENTS

45 BILLION NETFLOW SESSIONS FOR MALICIOUS ACTIVITY

[7] Level 3 internal research

WE SEE MORE, **SO WE STOP MORE**

Certified security professionals operate the Level 3 Threat Research Lab and our globally dispersed Security Operations Centers (SOCs).

DEVELOPING ACTIONABLE THREAT INTELLIGENCE +

LEVEL 3 THREAT RESEARCH LABS

Security specialists monitor communications between malicious actors and their victims, enabling us to predict risks, detect attacks and track zero day exploits.

REAL-WORLD SUCCESS

LEVEL 3 TAKES POSEIDON +

CLOSE ✕

LEVEL 3 THREAT RESEARCH LABS TAKES ON POSEIDON

PoSeidon, one of the most sophisticated recent examples of point-of-sale (PoS) malware, stole credit card data from compromised PoS systems and sent it to hackers in near real time. Level 3 Threat Research Labs monitored traffic to identify victims, isolated the attack's criminal origins, and worked quickly to reduce the impact of the attack.

READ MORE. +

REAL-WORLD SUCCESS

y to efficiently pond to icious or

EACH D SECURITY EXPERTS MONITOR AND N

200,000 ROUTE MILES OF FIBER GLOBALLY[7]

MALICIOUS PACKETS

45 BILLION NETFLOW SESSIONS FOR MALICIOUS ACTIVITY

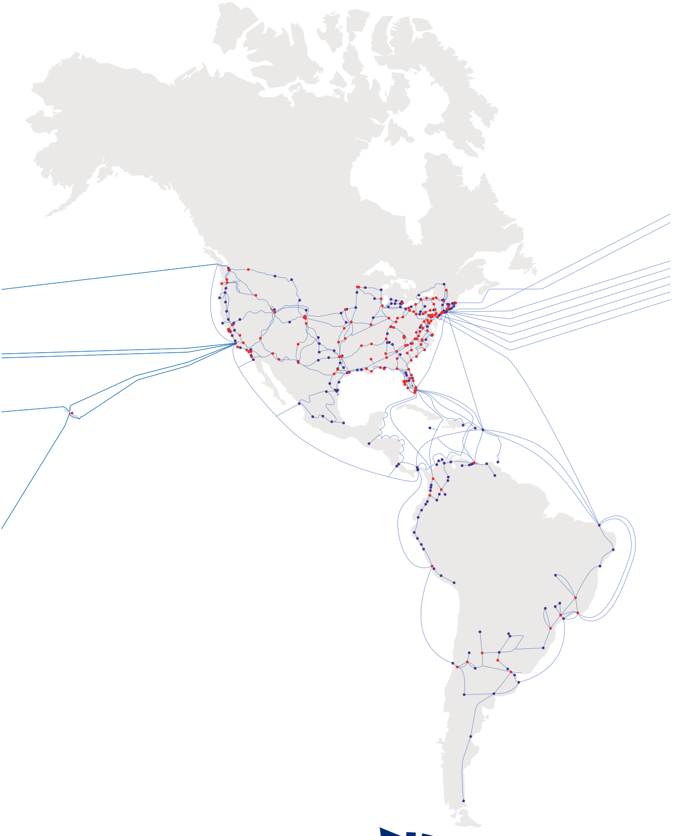
~1.3 BILLION SECURITY EVENTS

[7] Level 3 internal research

NETWORK-BASED SECURITY
OWN YOUR DEFENSE

Traditional point security solutions have had their day. But those reactive, isolated point solutions are simply unable to keep pace with the complexities of today's business environments and the evolving nature of threats.

Point solutions are labor intensive, needing to be individually managed and updated, and trying to get a complete picture of an organization's security posture is time consuming—if it can be done at all.



LEVEL 3 IS THE BETTER CHOICE FOR NETWORK-BASED SECURITY

Proactive, network-based security from Level 3 eliminates the complexity of point solutions and simplifies the management of your security profile. Level 3 will work with you make the transition to an outsourced model, helping you cut the costs of administration and reduce capital investment requirements—freeing budget and staff for other critical business needs.

WE MAKE THE CONVERSION TO NETWORK-BASED SECURITY EASY

Transition incrementally, to evaluate the service with very low risk. We'll identify the most efficient implementation strategy, while minimizing disruption through comprehensive support and guidance every step of the way.

BACKED 24X7 BY CERTIFIED, HIGHLY EXPERIENCED SECURITY PROFESSIONALS, NETWORK-BASED SECURITY SERVICES ARE AVAILABLE TO DELIVER A LAYERED DEFENSE THAT ENHANCES SECURITY AS BUSINESSES EVOLVE AND GROW.

NETWORK-BASED SECURITY **IN ACTION**

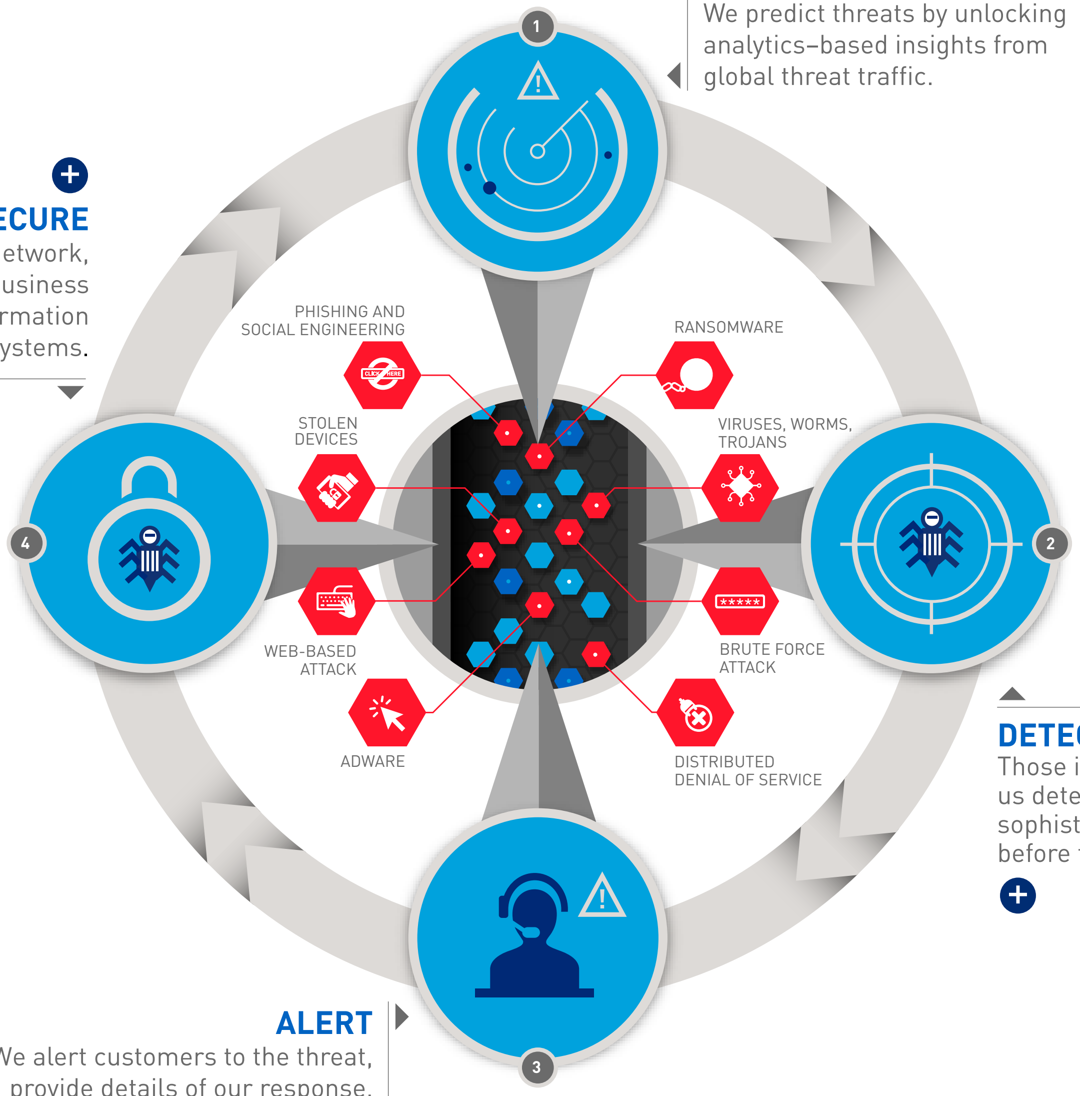
Network-based security from Level 3 is built around four essential actions:

PREDICT

We predict threats by unlocking analytics–based insights from global threat traffic.

SECURE

We secure the network, protecting your business critical information and systems.



DETECT

Those insights help us detect even the most sophisticated attacks before they occur.

ALERT

We alert customers to the threat, provide details of our response, and notify them of any further action they should take.

NETWORK-BASED SECURITY IN ACTION

Network-based security from Level 3 is built around four essential actions:

PREDICT

eats by unlocking
ed insights from
raffic.

SE

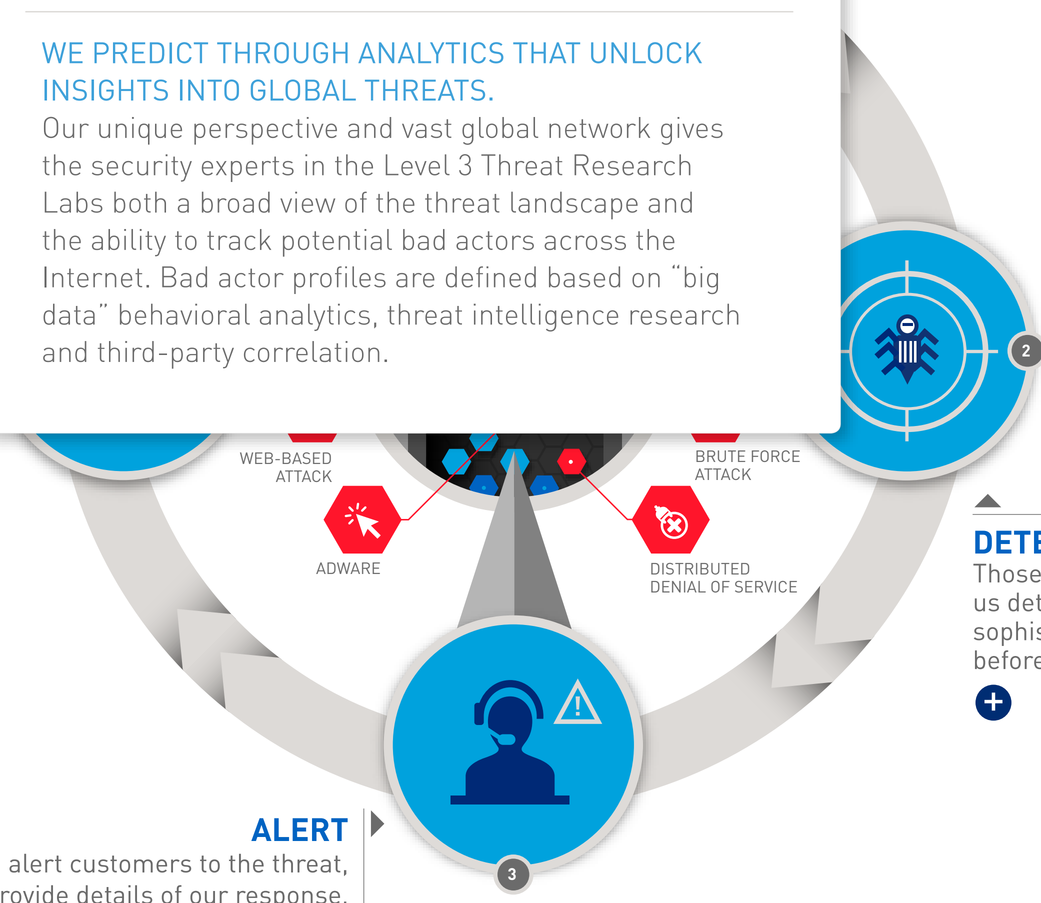
We secure the ne
protecting your bu
critical infor
and sy

CLOSE ✕

PREDICT

WE PREDICT 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.



DETECT

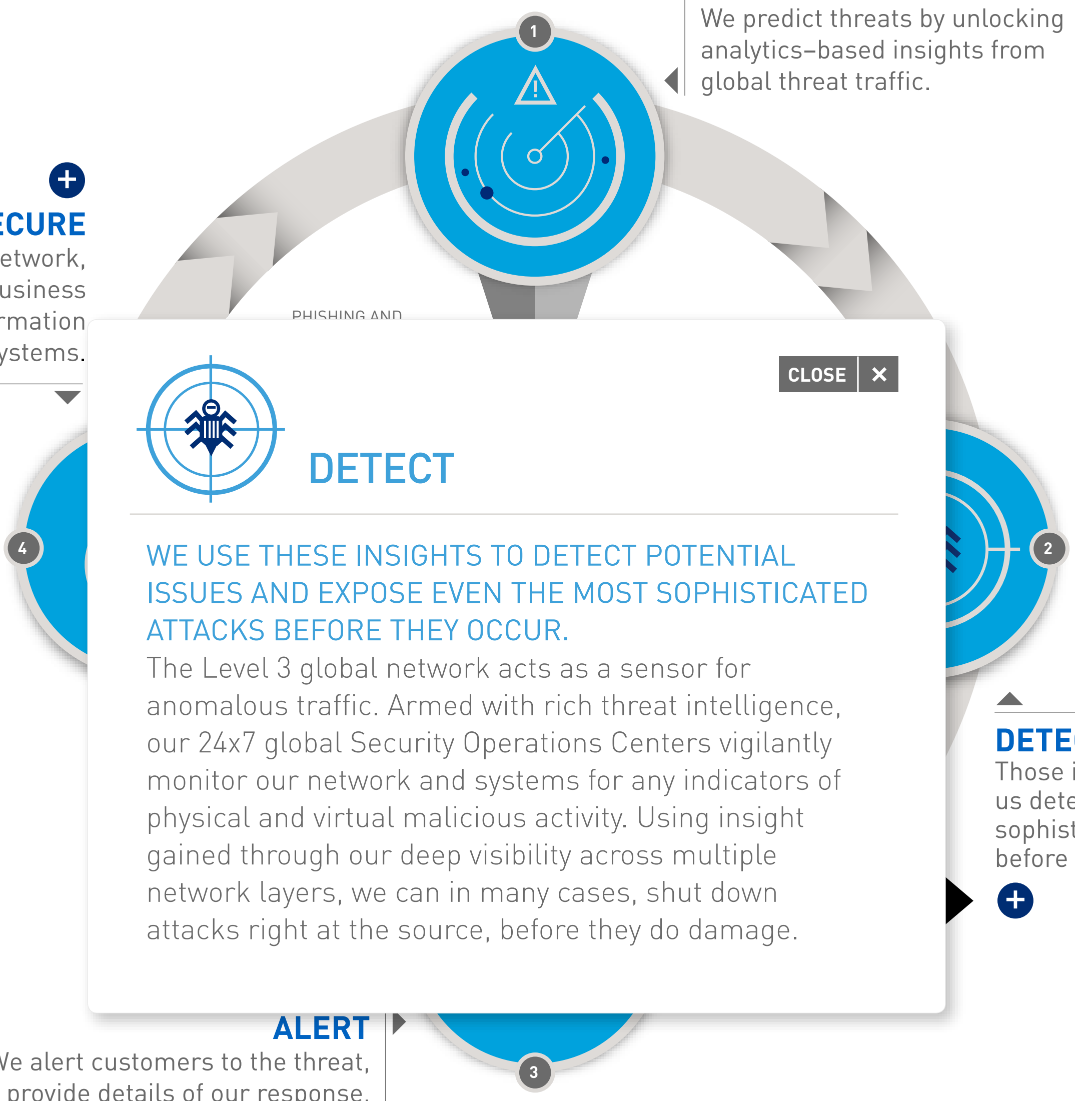
Those insights help us detect even the most sophisticated attacks before they occur.

ALERT

We alert customers to the threat, provide details of our response, and notify them of any further action they should take.

NETWORK-BASED SECURITY **IN ACTION**

Network-based security from Level 3 is built around four essential actions:



PREDICT

We predict threats by unlocking analytics–based insights from global threat traffic.

SECURE

We secure the network, protecting your business critical information and systems.

CLOSE ✕

DETECT

WE USE THESE INSIGHTS TO DETECT POTENTIAL ISSUES AND EXPOSE EVEN THE MOST SOPHISTICATED ATTACKS BEFORE THEY OCCUR.

The Level 3 global network acts as a sensor for anomalous traffic. Armed with rich threat intelligence, our 24x7 global Security Operations Centers vigilantly monitor our network and systems for any indicators of physical and virtual malicious activity. Using insight gained through our deep visibility across multiple network layers, we can in many cases, shut down attacks right at the source, before they do damage.

DETECT

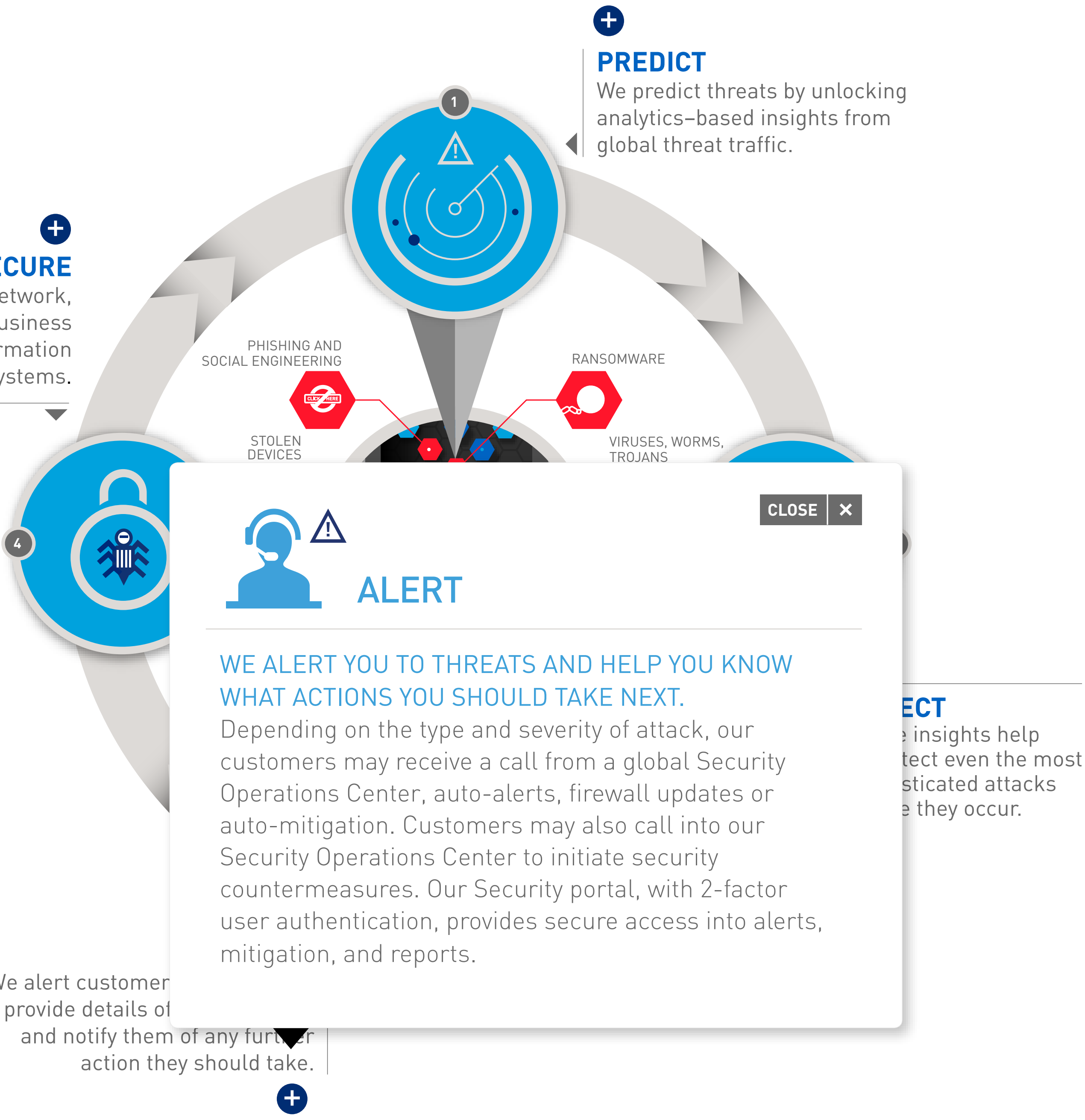
Those insights help us detect even the most sophisticated attacks before they occur.

ALERT

We alert customers to the threat, provide details of our response, and notify them of any further action they should take.

NETWORK-BASED SECURITY **IN ACTION**

Network-based security from Level 3 is built around four essential actions:



PREDICT
We predict threats by unlocking analytics–based insights from global threat traffic.

SECURE
We secure the network, protecting your business critical information and systems.

ALERT

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 a global Security Operations Center, auto-alerts, firewall updates or auto-mitigation. Customers may also call into our Security Operations Center to initiate security countermeasures. Our Security portal, with 2-factor user authentication, provides secure access into alerts, mitigation, and reports.

ECT
e insights help
tect even the most
sticated attacks
e they occur.

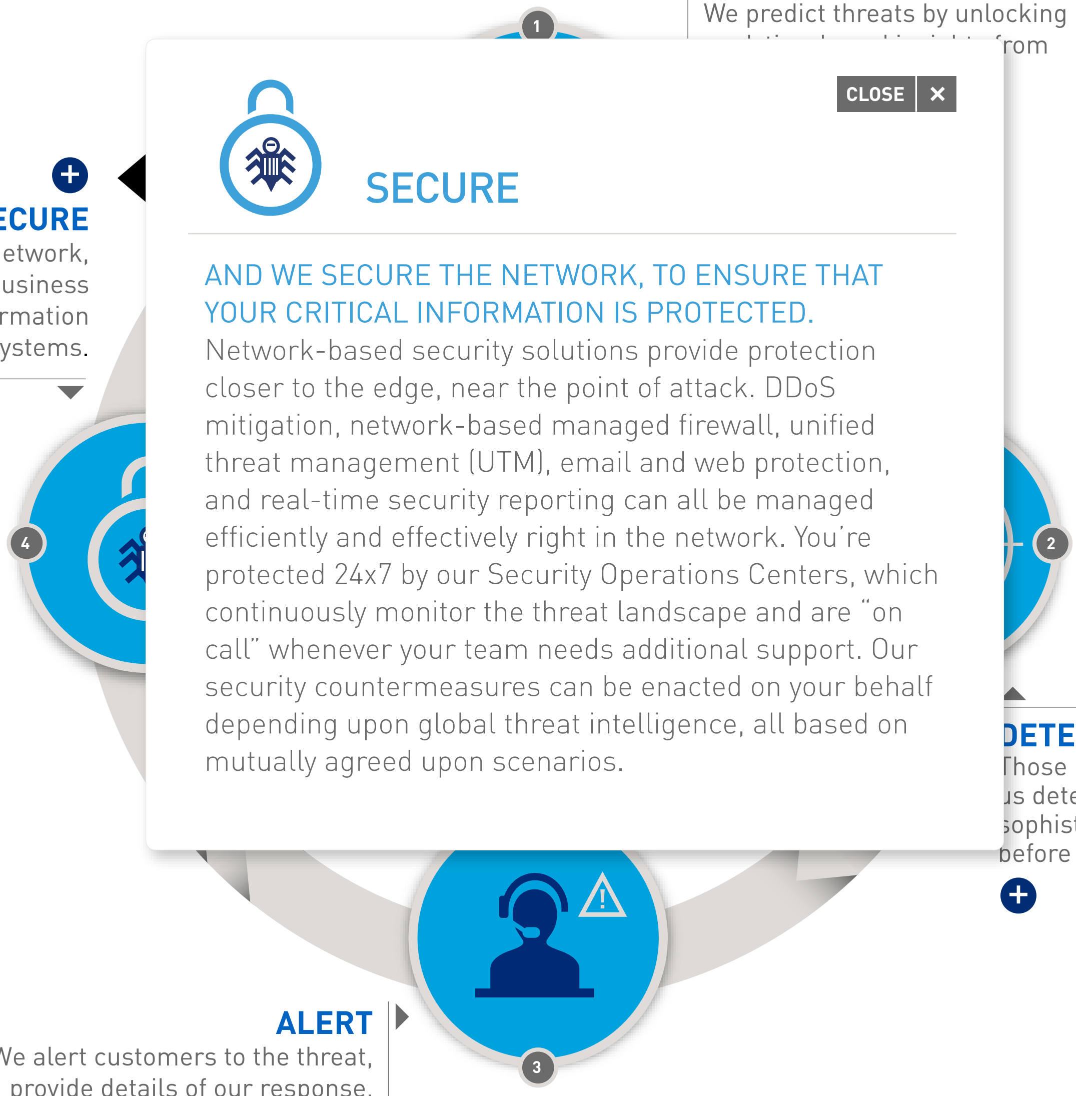
We alert customer
provide details of
and notify them of any furt er
action they should take.

NETWORK-BASED SECURITY **IN ACTION**

Network-based security from Level 3 is built around four essential actions:

PREDICT
We predict threats by unlocking
rom

SECURE
We secure the network, protecting your business critical information and systems.



CLOSE ✕

SECURE

AND WE SECURE THE NETWORK, TO ENSURE THAT YOUR CRITICAL INFORMATION 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. You're protected 24x7 by our 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.

DETECT
Those insights help us detect even the most sophisticated attacks before they occur.

ALERT
We alert customers to the threat, provide details of our response, and notify them of any further action they should take.

THE LEVEL 3 MANAGED SECURITY SERVICES PORTFOLIO

Level 3 is dedicated to providing you with 24x7 business continuity. The size and sophistication of our global network gives us access to a massive amount of security threat data, so we can help protect you from attacks before they affect your business.

SECURITY PROFESSIONAL SERVICES

THREAT INTELLIGENCE

LEVEL 3 EMAIL AND WEB DEFENSE

LEVEL 3 SECURE ACCESS SITE, MOBILITY AND CELLULAR SERVICES

DDOS MITIGATION SERVICE

LEVEL 3 MANAGED SECURITY SERVICES

BACK TO
THE LEVEL 3 MANAGED SECURITY SERVICES PORTFOLIO

SECURITY PROFESSIONAL SERVICES +

DDOS MITIGATION SERVICE +

LEVEL 3 EMAIL AND WEB DEFENSE +

LEVEL 3 SECURE ACCESS SITE, MOBILITY AND CELLULAR SERVICES +

LEVEL 3 SECURE ACCESS SERVICES +

THREAT INTELLIGENCE +

SECURITY PROFESSIONAL SERVICES

Defending against today's complex security threats requires a dedicated team of specialists. By drawing on expertise and insight gained from serving a global customer base and managing a diverse fiber network, we will develop a comprehensive security plan that enables your business to operate with confidence wherever you choose.

KEY FEATURES

- Identifies areas of concern through penetration testing and vulnerability assessments
- Defines a security strategy that maps security policy to critical applications, corporate culture, staff, processes and technologies
- Augments your security blueprint to include a recommended plan, set of priorities and expected return on investment (ROI)
- Measures results and value creation
- Provides a trusted security advisor every step of the way

BENEFITS

- Provides unbiased advice on the state of your current security posture
- Delivers a clear roadmap and detailed action plan for improving your network security
- Enables rapid return on investment

◂BACK TO
THE LEVEL 3 MANAGED SECURITY SERVICES PORTFOLIO

SECURITY PROFESSIONAL SERVICES +

DDOS MITIGATION SERVICE +

LEVEL 3 EMAIL AND WEB DEFENSE +

LEVEL 3 SECURE ACCESS SITE, MOBILITY AND CELLULAR SERVICES +

LEVEL 3 SECURE ACCESS SERVICES +

THREAT INTELLIGENCE +

LEVEL 3 DDOS MITIGATION SERVICE

Today's highly sophisticated distributed attacks require more than typical scrubbing center mitigation techniques. Our network-based DDoS mitigation solutions defend enterprise resources through a multi-layered security approach backed by extensive threat research.

KEY FEATURES

- Provides 4.5 Tbps of attack ingestion capacity
- Can be paired with network protection services that includes routing, filtering and rate limiting
- Enables reroute and scrubbing of all Internet connections, not just Level 3 on-net capacity
- Connect via GRE, Proxy or more than 250 multiprotocol label switching (MPLS) points of presence (POPs) globally

BENEFITS

- Leverages Level 3 threat intelligence capabilities, based on our global IP networks, content delivery networks (CDNs) and domain name server (DNS) networks, which enable unique visibility into attack traffic and emerging threats
- Helps ensure business continuity and safeguard brand reputation, by keeping critical assets and systems up and running
- Simplifies operations, through network-based, carrier-agnostic service with a single point of contact for threat resolution

◀BACK TO
THE LEVEL 3 MANAGED SECURITY SERVICES PORTFOLIO

SECURITY PROFESSIONAL SERVICES +

DDOS MITIGATION SERVICE +

LEVEL 3 EMAIL AND WEB DEFENSE +

LEVEL 3 SECURE ACCESS SITE, MOBILITY AND CELLULAR SERVICES +

LEVEL 3 SECURE ACCESS SERVICES +

THREAT INTELLIGENCE +

LEVEL 3 EMAIL AND WEB DEFENSE

Block attacks from the network's edge with easy-to-deploy, cloud-based defensive services. We provide always on email and web protection, safeguarding your employees and helping them stay productive—wherever business takes them.

KEY FEATURES

- Protects inbound and outbound emails with multilayered protection that includes spam, malware, reputation, virus, worm, content, attachment and email attack filters
- Helps ensure email continuity, even if email systems go offline
- Utilizes email encryption technologies and strategies with advanced data loss prevention and compliance capabilities
- Provides content scanning, document fingerprinting and transport layer security
- Delivers a strong and reliable web defense, with protections against dynamic web-based malware via advanced web filtering technology

BENEFITS

- Scales easily to support organizations of any size
- Simplifies management of email and web security policies through an intuitive administrative console
- Ensures continuity, keeping your email systems safe and available

◀ BACK TO
THE LEVEL 3 MANAGED SECURITY SERVICES PORTFOLIO

SECURITY PROFESSIONAL SERVICES +

DDOS MITIGATION SERVICE +

LEVEL 3 EMAIL AND WEB DEFENSE +

LEVEL 3 SECURE ACCESS SITE, MOBILITY AND CELLULAR SERVICES +

LEVEL 3 SECURE ACCESS SERVICES +

THREAT INTELLIGENCE +

LEVEL 3 SECURE ACCESS SITE, MOBILITY AND CELLULAR SERVICES

Moving managed firewalls and UTM into the network helps you to simplify security infrastructure and operations, while reducing costs. And with gateways on four different continents, we offer a low latency access option for improved Internet speeds and quick application response times.

KEY FEATURES

Delivers the protections you need most:

- 24x7 proactive monitoring and alerts
- Firewall
- Premises or cloud-based deployments
- Intrusion protection
- Web content filtering
- Antivirus/Anti-spam
- Real-time security reporting

BENEFITS

- Scales easily and cost effectively to support networks regardless of size, number of sites, traffic volumes or geographic location
- Controls both capital expenditures and operating expenses, while providing predictable monthly costs and freeing staff for other projects
- Simplifies IT management by providing Level 3 experts, knowledge, systems and technologies that deliver “always on” Internet security
- Defends against a wide range of malware and attack types, helping secure your Internet connections from threats to business-critical applications, systems and endpoints

◀BACK TO
THE LEVEL 3 MANAGED SECURITY
SERVICES PORTFOLIO

SECURITY PROFESSIONAL SERVICES +

DDOS MITIGATION SERVICE +

LEVEL 3 EMAIL AND WEB DEFENSE +

LEVEL 3 SECURE ACCESS SITE, MOBILITY AND CELLULAR SERVICES +

LEVEL 3 SECURE ACCESS SERVICES +

THREAT INTELLIGENCE +

LEVEL 3 SECURE ACCESS SERVICES

Our dedicated team of certified security specialists provides 24x7 monitoring and threat analysis of your security appliances for a complete view of security incidents. And we'll keep your network safe—without sacrificing accessibility.

KEY FEATURES

Three options are available:

- **Site option:** Extends virtual private network (VPN) access to small or remote offices with a basic Internet connection, and helps ensure data remains unmodified and private while in transit.
- **Mobility option:** Securely connects remote users or teleworkers to networks, critical data and applications via laptops, tablets or smartphones
- **Cellular option:** Provides secure 4G/LTE cellular connectivity for small remote sites, providing backup in the event of primary VPN connectivity failure.

BENEFITS

- Delivers confidence through continuous protection of your sensitive data
- Solutions managed and monitored 24x7 by our security experts, which frees resources, so your team can focus on growing your business
- Drives better productivity by giving employees safe, secure network access from anywhere, on any device

THREAT INTELLIGENCE

Our comprehensive vantage point and global footprint enables us to monitor massive Internet traffic volumes for malicious activity. We can help you identify threat communications before they infiltrate your data, systems and network.

KEY FEATURES

- Provides threat impact reporting that gives insights on botnet behavior, DDoS attack patterns and other vulnerabilities
- Speeds research into geographic trends, victim and successful attacker profiles, and discover why tracking two-way communications is critical for mitigating evolving cyber threats.

BENEFITS

- Reveals where threats originate, through regular monitoring of known command and control servers, as well as malware and phishing domains
- Tracks traffic to detect abnormal spikes that are a leading indicator of cyber threats
- Helps defend against social engineering, using techniques that focus on intelligent, role-based targeted attacks

◂BACK TO
THE LEVEL 3 MANAGED SECURITY SERVICES PORTFOLIO

SECURITY PROFESSIONAL SERVICES +

DDOS MITIGATION SERVICE +

LEVEL 3 EMAIL AND WEB DEFENSE +

LEVEL 3 SECURE ACCESS SITE, MOBILITY AND CELLULAR SERVICES +

LEVEL 3 SECURE ACCESS SERVICES +

THREAT INTELLIGENCE +

DEFEND YOUR BUSINESS WITH NETWORK-BASED SECURITY FROM LEVEL 3

Greater protection than traditional point security solutions. Less complexity. Simpler management. It's time for network-based security from Level 3.

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

And, if you're currently planning your next network expansion, this may be the perfect time to make the switch. We can implement network-based security on just the expanded network area only, so you can experience the benefits firsthand, before rolling out this improved protection across the organization.

LEARN MORE ABOUT NETWORK-BASED SECURITY, OR OTHER LEVEL 3 SECURITY SERVICES, AT:

www.level3.com +

Connecting and Protecting
the Networked World®

TAKE CONTROL OF YOUR NETWORK SECURITY.
OWN YOUR DEFENSE.