

WHITE
PAPER

Managing to the Edge

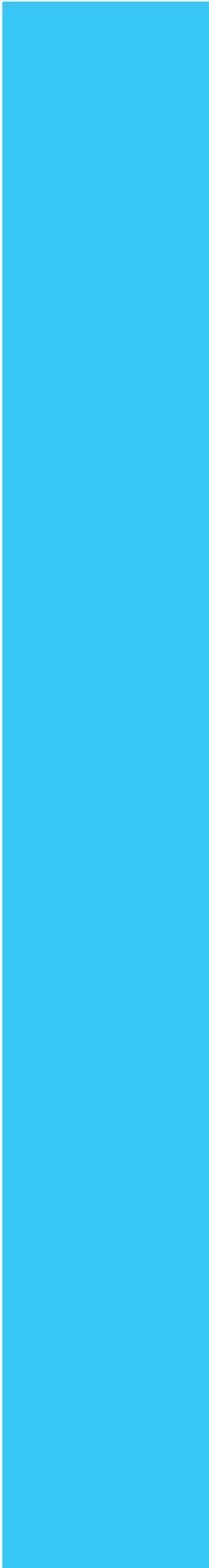
The Necessity of
Network-Integrated Security.

Security leaders report quantifiable success, significant value, and improvements in business outcomes with third-party managed services.

SPONSORED CONTENT

CSO
FROM IDG

LUMENSM



IT and security leaders cite significant improvements and a high level of confidence in their cybersecurity posture thanks to managed network security services, according to a new IDG study. For example, companies using third-party services to integrate essential network security technologies report:

- Shorter response times—up to 49%—to remediate threats
- Improvements in efficiency of incident response—up to 38%—and system availability—up to 46%
- Reduction in false positives—up to 50%
- Reduction in compromised devices—up to 39%—and security events—up to 38%—that require investigation

The results are promising—especially in light of ongoing security talent shortages, as well as the data tsunami and growing bandwidth requirements at the edge, which place even more pressure on network capacity and performance.



The key to success is having an integrated network security strategy, rather than bolting on solutions in a piecemeal fashion.

“Security is an inherent ingredient in networking today,” says Chris Betz, CSO at Lumen. “It must be baked in at the beginning, not added on in isolation. For example, it doesn’t make sense to deploy an antivirus solution for each new IoT device. You need an integrated security strategy from the start.”

This report examines the results of an IDG survey of 351 IT security leaders, including their quantified improvements in four critical areas of managed security services:

- Threat intelligence
- Security information and event management (SIEM)
- Cloud-based distributed-denial-of-service (DDoS) mitigation
- Managed firewalls

This report also looks at what’s ahead and explores how companies can best integrate network-based security technologies across their organizations.

Threat intelligence

Critical visibility for a dynamic attack surface

The more threats you can see, the more you can stop. And the greater the visibility, the faster these threats can be stopped before they become business-impacting events.

It’s more urgent than ever to have these threat insights, because the attack surface is expanding, writes Joel Oltsik, a principal analyst at Enterprise Strategy Group (ESG). “For example, we are seeing attacks on cloud infrastructure like the theft of developer passwords on Github, break-ins on Amazon S3 buckets, and exploitation of Internet of Things (IoT) device vulnerabilities. None of the adversary tactics, techniques, and procedures (TTPs) are new, but the cybersecurity diaspora is being asked to safeguard more new stuff all the time.”

The problem is, threat intelligence on its own doesn’t have true impact unless that data is actionable. Even without considering the ongoing cybersecurity talent scarcity, most companies don’t have the resources to manually sift through and correlate mountains of data, let alone ensure that they’re focusing on the right feeds and alerts. That’s why enterprises are increasingly adopting managed threat intelligence platforms to better understand insights across internal and external threats and to help prioritize incident response.

Those that have deployed such platforms are seeing staggering success: 99% of IT leaders using third-party threat intelligence say they’ve recorded notable improvements (see Figure 1), with 39% citing significant gains. In terms of the degree of business outcome improvement:

- 51% cite a significant increase in the ability to identify threats earlier in the kill chain
- 43% cite significant improvements in reducing blind spots

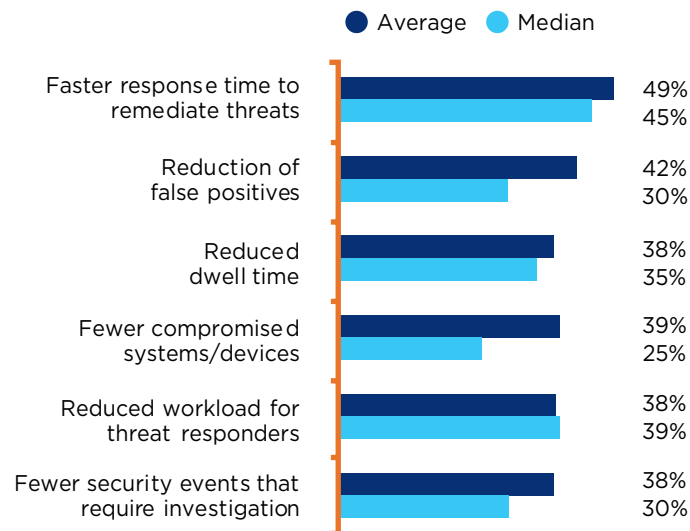
“Companies are finding that they have to go to a third-party not only to get that broad visibility into threats,” says Betz, “but, more importantly, to turn that information into actionable insights.”

The three most significant KPI improvements for third-party managed threat intelligence are:

- 45% to 49% faster response time to remediate threats
- 30% to 42% reduction in false positives
- 35% to 38% reduction in dwell time

F1

Third-party managed threat intelligence platforms offer multiple KPI improvements



SIEM

Enabling rapid threat detection and response

The explosion of data at the edge is evident. With the development of new applications and devices, including the rise of IoT, the world is expected to daily generate 463 exabytes of data by 2025.

Both IT and the business are pressured to deal with this volume at speed, especially by competitive forces such as the need to support real-time customer experiences. Right around the corner, 5G will further impact data traversing the network.

The protective umbrella for the network is a SIEM, a core technology that monitors, analyzes, and correlates data logs for anomalies and potential cyberthreats. Today's organizations can't hire or scale their way out of the inability to handle an increase in alerts. They need more intelligence behind data generated from systems and logs, and the ability to increase visibility across disparate and hybrid network elements.

The constant, evolving need for context is what makes SIEM challenging. “Something might look odd within your enterprise’s data, but it’s normal for your industry,” explains Betz. “It requires a niche skill set. There are advantages to using a managed service that can look for anomalies against what’s happening across industries and communities.”

F2

Third-party siem systems improve multiple security KPIs



To overcome data overload, manually intensive processes, and limited expertise, companies are shifting their SIEM management to third parties. Among those using such services, 96% report across-the-board improvements (see Figure 2).

The three most significant KPI improvements for third-party managed SIEM systems are:

- 35% to 40% shorter time to uncover active threats and potential indicators of compromise (IoCs)
- 30% to 39% reduction in dwell time
- 30% to 38% improved efficiency for incident response

Cloud-based DDoS mitigation

Balancing network performance and mitigation with fast recovery

DDoS attacks have been steadily increasing over the years, growing more sophisticated and larger. Many attacks are executed by cybercriminals who are testing defense capabilities or using the attack as a distraction from other targeted malicious activity.

For example, “in the mid-1990s, [a DDoS] attack may have consisted of 150 requests per second—and it would have been enough to bring down many systems. Today they can exceed 1,000 Gbps. This has largely been fueled by the sheer size of modern botnets,” according to CSO.

Most companies find it challenging to combat volumetric attacks like this. “You need significant ingest capacity and diverse scrubbing capabilities from your mitigation provider,” Betz explains.

DDoS mitigation is a necessity. One such attack can cripple a business and impact downstream customers if web-facing systems and applications aren’t recovered quickly.

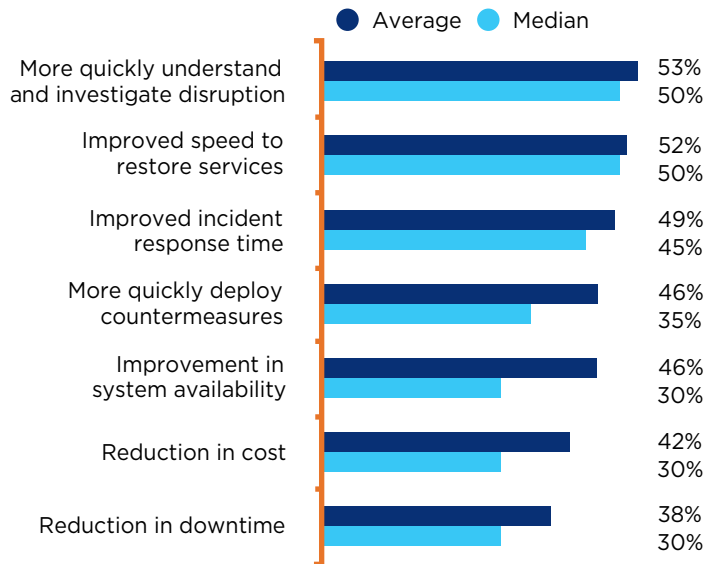
Enter cloud-based DDoS mitigation versus on-premises solutions. The former better meets the need for greater speed to deploy countermeasures and restore services. After implementing third-party cloud-based DDoS mitigation, 97% of IT leaders have reported improvements in areas such as system availability, incident response time, and reduced downtime, along with impressive KPI results (see Figure 3).

The three most significant improvements for third-party cloud-based DDoS mitigation are:

- 50% to 53% shorter time to understand and investigate disruption
- 50% to 52% improvement in the speed to restore services
- 45% to 49% shorter incident response time

F3

KPI improvements associated with third-party managed, cloud-based DDoS mitigation



Managed firewalls

Improving on a table stakes technology

Firewalls have been a standard network defense technology for decades. Yet, as the traditional network has expanded to the cloud, new measures are necessary for today’s more complex, hybrid computing environments. Enterprises must ensure that consistent policies are deployed across endpoints and critical locations while meeting evolving threats.

Firewall management is ripe for managed services. Imagine a security professional evaluating threat intelligence or monitoring SIEM logs when a threat alert comes up.

“You really don’t want that person to have to pivot and go deal with the firewall to block that traffic,” Betz says. “The complexity of managing firewalls—where you have inbound traffic over wireless and wired networks at massive volumes—means that the scale at which you have to operate it is enormous. This is exactly the place where you go to the experts and buy a skill set that already exists, so you can focus your limited resources on the areas that are unique to you.”

The IDG survey confirms that this is the tactic IT leaders are taking. Of those that have deployed third-party managed firewalls, 40% have cloud-based solutions, 25% have on-premises solutions, and 35% are using a combination of both. Among the advantages of cloud-based deployments are higher availability, scalability, and extensibility. Achieving these benefits on-premises would require increased capex and opex investments.

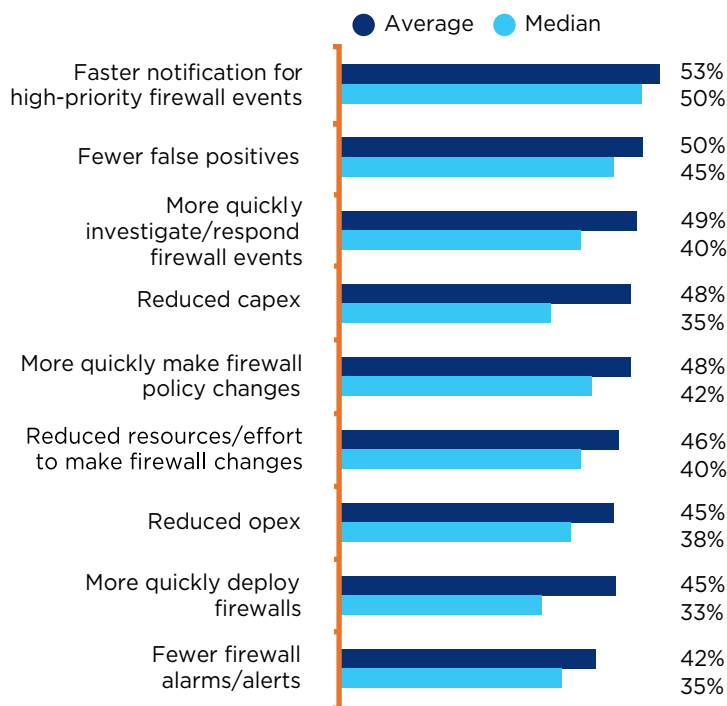
Significantly, 97% of the respondents to the IDG survey see improvements with third-party managed firewalls, most notably in terms of the ability to free up resources to focus expertise elsewhere (54%) and a better security posture (42%)—along with well-rounded results (see Figure 4).

The three most compelling KPI improvements for third-party managed firewalls are:

- 50% to 53% faster notification for high-priority firewall events
- 45% to 50% reduction in false positives
- 40% to 49% faster response to investigate firewall events

F4

The many benefits of third-party managed firewalls



Next on security leaders' agenda

Automation

Having achieved significant results with managed services, IT leaders are ready to double down on business outcomes by applying automation. Over the next three years, they expect that automated threat detection and remediation will improve their organizations' security posture.

Specifically, leaders anticipate reducing the burden on IT, better meeting security outcomes, and gaining business efficiencies (see Figure 5).

Automation is about scalability, Betz says. From a cultural standpoint, it makes sense: "If a computer can do it, then the computer ought to do it, so your teams can be doing work with higher impact."

The biggest challenge, he adds, is control—ensuring that the system understands what to ignore and what to pay attention to. He advises a feedback loop, such as a red team, to scope out effectiveness and potential issues.

At the end of the day, automation should ultimately be about empowering people, giving them the tools to "control their own fate, make their work and their jobs better, and make their customers better," Betz says.

Considerations for an integrated security strategy

The results of the IDG survey demonstrate the significant value that can be achieved with third-party managed network security solutions. Companies evaluating managed services for network security should ask themselves three questions:

1. Does it improve security?

If this is an area where your company already does security well, you should double down on your expertise. Otherwise, rely on a third party with an in-depth focus.

2. Does it reduce friction?

With the limited amount of security talent, internal experts can't be fighting the system. If security is making their jobs harder, employees will find a way to go around it. So a managed solution needs to reduce day-to-day friction.

3. Does it decrease costs?

Security teams must demonstrate the value they bring to the company. With limited funds, investment in security controls must be balanced with the need to run the business.

What's more, it's becoming urgent to make these strategic decisions, Betz notes. "We're facing an onslaught of data, the increasing adoption of IoT, and 5G around the corner. It's time to wrap managed third-party solutions into an integrated security strategy."

A holistic, integrated strategy means ensuring that security solutions fit into the existing network to extend visibility across the organization. It cannot be a patchwork of disparate, bolted-on solutions that businesses are left to stitch together on their own.



F5

IT security leaders outline anticipated benefits of automated threat detection and remediation



Reducing the burden on staff

“By freeing IT staff from day-to-day general threat activities, we can concentrate resources on process improvements.”

“It will help significantly reduce the time and manpower needed to improve our risk management.”

“It will enable us to move to other items that require our attention. We’ll be able to concentrate on bigger issues.”

“It allows us to focus on other security aspects with no loss of confidence.”



Improving security outcomes

“My hope is that it will be better at keeping information secure and detecting when someone is trying to hack into the system.”

“It will significantly speed up the process of detecting and resolving threats and require less oversight.”

“It will give us the ability to stop or prevent intrusions and disruptions to our business from viruses and unwanted intrusion into our system.”

“It will allow us to concentrate on the real threats.”



Improving business outcomes

“Increased coordination of systems will enhance our total threat response and continue to improve our position across all categories and pain points.”

“It will help us be more compliant. I think we will gain more trust with our customers as our data protection constantly improves.”

“I think it will increase the overall morale of the company.”

“It will improve our operations and how we do business.”

Unique success

Notable KPI achievements by industry

Although all respondents in the IDG study reported improvements to their security posture as a result of third-party security services, a few industry distinctions bubbled up. For example, healthcare companies were more likely to report “significant”—versus moderate or modest—overall improvements.

All respondents were asked to quantify enhancements on a scale of 0% to 100%. IDG averaged their responses. Significant KPIs are illustrated in the tables below.

No matter the industry, there are advantages to investing in third-party managed security services.

To determine the best path forward, “double down on areas where you’re unique,” says Betz. “also, as you make improvements in one area, share those insights with your managed services partners and seek opportunities to work better together. The more you put in, the more you get out.”

About the Survey

To better understand the impact of third-party managed security technologies, IDG surveyed 351 U.S.-based IT security leaders at companies with more than 500 employees. Participants represented the following industries: healthcare (25%), manufacturing (16%), financial services (16%), retail (14%), business services (4%), architecture (4%), and education (3%).

To qualify, respondents had to be involved in vendor evaluation, selection, purchase, and/or implementation for one or more of the following technologies: third-party managed threat intelligence; third-party managed SIEM system; third-party managed cloud-based DDoS mitigation; and/or third-party managed firewalls. Lumen sponsored the survey, which was conducted online May 10–22, 2019, and July 29–August 2, 2019.

Significant improvements from third-party services (by industry)

	Threat intelligence	SIEM	Cloud-based DDoS	Firewalls
Financial Services	29%	34%	60%	36%
Healthcare	45%	40%	41%	48%
Manufacturing	33%	28%	35%	40%
Retail	38%	29%	43%	34%

Areas showing greatest gains within specific industries

Threat intelligence	<ul style="list-style-type: none">• 50% reduction in compromised platform systems/devices (retail)• 55% reduction in dwell time (financial services)
SIEM	<ul style="list-style-type: none">• 60% improvements in uncovering active threats (retail)• 47.5% reduction in dwell time (healthcare)
Cloud-based DDoS mitigation	<ul style="list-style-type: none">• 85% improved speed to restore services (manufacturing)• 60% improved time to understand and investigate disruptions (financial services)• 75% shorter time to deploy countermeasures (manufacturing)
Managed firewalls	<ul style="list-style-type: none">• 75% reduction in capex and 70% average reduction in opex (healthcare)• 75% reduction in false positives and 65% improved notification speed for high-priority events (manufacturing)



The inherent value of connected security

Connected Security is our vision for the seamless integration of security and the network to transform the future of communications. At Lumen, our approach to security is founded on two fundamental principles: to leverage our expansive visibility into the global threat landscape and to take action against the threats we see. With the unique and deep network-based threat intelligence of our threat research and operations arm, Black Lotus Labs, we have transformed our network into a threat sensor and proactive defense platform. This is what makes Connected Security possible.

Disclaimer

This document is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided “as is” without any warranty or condition of any kind, either express or implied. Use of this information is at the end user’s own risk. Lumen does not warrant that the information will meet the end user’s requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen’s products and offerings as of the date of issue.