Infoblox
CONTROL YOUR NETWORK

2016 Network Protection Survey

"We control the electrical grid for 13 states. When the grid goes down it affects millions of people. In some cases it is a life and death issue. Without a doubt, network protection is really, really important to us."

– Network Analyst, Major Public Utility, Northeastern United States

Networks, more than ever, are at the core of the enterprise. Analysts estimate the cost of a typical unplanned network outage now tops $740,000[1]. Protecting the network – from problems like breaches, outages and poor performance – is crucial for organizations.

Infoblox wanted to explore how organizations are protecting and managing their networks in today's chaotic world. We commissioned ReRez Research of Dallas, Texas, to survey 200 large organizations to discover network protection best practices and how adherence to these industry best practices affect eventual outcomes.

We were able to discover precisely what the very best organizations were doing to protect and manage their networks, and how these practices affected their outcomes. From this, we are able to make five recommendations for organizations trying to protect their networks in today's complex and chaotic world.

[1] Ponemon Institute 2016 report Cost of Data Center Outages

Think strategically

Our first insight into how the top-tier differs from the bottom-tier came while analyzing their goals and objectives. Top-tier IT professionals focus on strategic goals while bottom-tier IT focuses on more tactical issues.

Top-tier's top two goals are IT agility and making IT a strategic asset for their organization whereas bottom-tier focuses on security and lowering IT costs.

"Our days are filled with a whirlwind of activity, which can make it hard to work on strategic initiatives," says a system engineer for a large top-tier technology company in Florida. "To combat that we all choose a one-year strategic goal that will improve our organization. We have tangible milestones we commit to and are responsible for throughout the year. This helps us stay strategic and deploy exciting next-generation initiatives that help make us a better organization."

By contrast, a network analyst for a bottom-tier organization in New York laments "We just don't have much time to even think about next-gen stuff, or even to improve of what we already have."

As we'll see in a moment, this difference in how the top-tier approaches goals has a significant impact on their outcomes.

TOP TIER

- IT Agility
- Making IT a strategic asset
- Compliance

BOTTOM TIER

- Security
- Reducing IT Costs
- Compliance

What are top-tier IT organizations doing differently

It is hard enough to protect against the advanced threats aligned against today's network. It is an order of magnitude more difficult when IT lacks visibility into basic things like which devices are on the network, what threats are out there and where your network is vulnerable.

PROACTIVE ABOUT INTELLIGENCE

Four times as likely to leverage machine-readable intelligence

Six times as likely to deploy an SEIM solution, and use automated tools that alert them when new devices appear on the network

HAVE BANISHED SILOS

100% report cooperation between network, security and app teams

Only 43% report similar cooperation

VALUE DNS/DHCP DATA

Roughly half use DNS/DHCP data to discover new devices

49%

0%

Verses NONE for the bottom-tier

AUTOMATE BASIC TASKS

Three to four times as likely to automate routine tasks

INVEST IN SECURITY STAFF

Three times less likely to report being understaffed

58%

More than half have a dedicated incident response team

33%

Verses one-third of the bottom-tier

A senior network engineer with a large healthcare organization in the New York City area says security is not an IT priority, it's an organizational one. He adds that, "(we) are extremely committed to this, and it gets full attention from upper management. Ensuring information security is not just the law, it's critical to the reputation of the company."

Commitment to Security Intelligence

One of the ways the top-tier attacks this problem is with security intelligence. Which devices are on your network? Top-tier is **six times** as likely to use an automated tool that alerts them when new devices appear on the network. They are **six times** as likely to have deployed a security information and event management solution (SIEM). Finally, they are **four times** as likely to invest in machine-readable threat intelligence. A senior engineer for a tech warranty support provider with over 30,000 users calls his company's decision to focus on security a difference-maker, adding "Our security auditing policy team has probably eight to 10 times larger than it was two years ago, and our focus has come around 180 degrees in the last two or three years. A primary concern is identifying attack avenues that we've never really done anything with."

Banish Silos

Top-tier organizations are also much less tolerant of silos – either in their tools or in their teams. They are nearly **nine times** as likely to use integrated visibility tools, **four times** as likely to use integrated security tools and fully **100 percent** report moderate to complete cooperation and coordination between their network, security and app teams (versus less than half of the bottom-tier).

Often, these silos are not formed consciously. A network engineer for a large technology support company in the Southern U.S. commented, "IT shops are running so lean these days, even just knowledge transfer is prohibitive. Silos often form simply because we don't have time to share."

Leverage DNS and DHCP Data

One tactical difference between the top and bottom-tier organizations is how much they leverage DNS and DHCP information to help protect their network. The top-tier places a very high value on this data. In fact, **roughly half** the top-tiers use such data to discover new devices on the network (versus none of the bottom-tier). Top-tier is nearly **three times** as likely to use DNS logs for security purposes. And, not surprisingly given the value they place on DNS data, the top-tier is **twice** as likely to use purpose-built DNS server safeguards.

A senior systems engineer for a large healthcare organization that has 400,000 IP address spread over three continents explains, “We began analyzing DNS data maybe three or four months ago. What we saw has been incredible. We have been discovering all manner of suspicious activity – it is just off the scale.”

Automate Basic Task

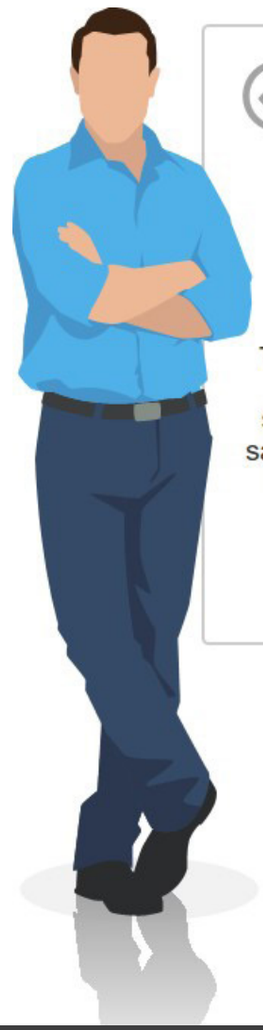
The top-tier also automates much of their basic network tasks. Virtually **all** the top-tiers have precise configuration and security requirements defined for their network devices compared to just 29 percent of bottom-tiers. Furthermore, they are **three** to **four times** as likely to have automated such routine tasks as setting security configurations for new apps, for configuring network devices, achieving compliance and deploying new apps or services.

Investing in Security

Finally, in keeping with the top-tier’s focus on strategic goals, they are much more likely to invest in security. In fact, they are **three times** less likely to report being understaffed for security. Most **(58 percent)** also have a team dedicated to incident response, whereas two-thirds of the bottom-tier do not.

Top-tier IT organizations enjoying significantly better outcomes

Top-tier IT organizations employ industry best-practices when it comes to network protection. Does that help? Our research shows that it does – **dramatically.**



CUSTOMER EXPERIENCE

Top-Tier IT is two times as likely to have somewhat to extremely satisfied compatriots from the business, the "C"-level and users alike

RISK MANAGEMENT

zero

Bottom-tier report three security-incident related outages while top-tier report zero

zero

Data breach: Top-tier zero, bottom-tier one

OPERATIONAL EFFICIENCY

Twice as likely to meet SLAs

Ten times as likely to remediate security events "extremely quickly"

BETTER VISIBILITY

Four times as likely to report having complete control over their IP addressing

MORE AGILE

More than twice as likely to say they focus more on strategic tasks than tactical

Customer Service

The top-tier is much more likely to be held in high-regard by their organization – roughly **twice as likely** to have somewhat to extremely satisfied compatriots from the business, the “C”-level and users alike.

Risk Management

While bottom-tier organizations reported three security-incident related outages and one data breach, top-tiers reported **none**. Top-tiers are also much more likely to achieve internal and external compliance.

A systems and network administrator with a public high school district outside Chicago says his team used to struggle with denial-of-service attacks. The district issues students iPads, and all of those wireless devices connecting to the network made identifying the attacks avenues difficult. “We weren’t sure if the students were initiating them by paying websites to do it, or if we had malware on machines that the bots were use using to phone home and attack us. But after we implemented DNS security, we’ve had no more denial-of-service attacks. We were then able to see what machines were actually trying to connect back to our servers. We either removed the malware or re-imaged those machines, and that solved our issues.”

Smoother Operational Efficiency

The ultimate benefit for the top-tier is that their networks just run more smoothly. They are roughly **twice** as likely to meet SLAs and **ten times** as likely to remediate security events “extremely quickly.”

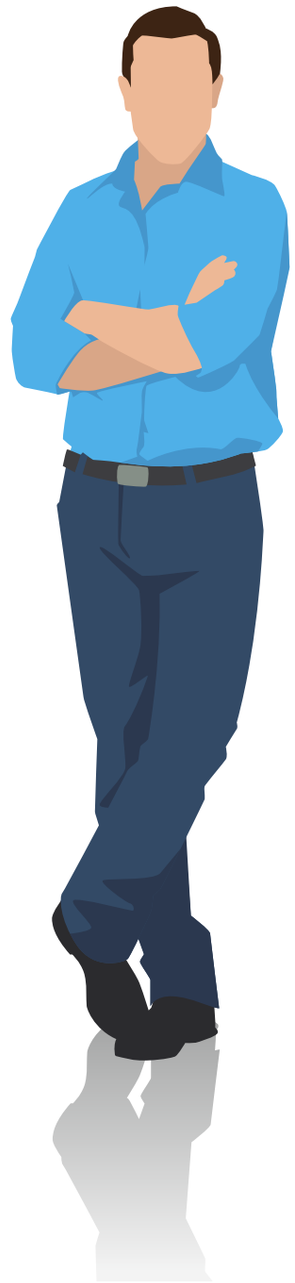
Better Visibility

As mentioned earlier, effective network protection requires superior visibility. The top-tier has significantly better visibility into and control over infrastructure details such as IP addresses, malicious DNS traffic, and trusted users deviating from appropriate behavior. This can be seen in the fact that the top-tier is **four times** as likely to report having complete control over their IP addressing.

Agile and Strategic

In keeping with their stated goals, top-tier organizations are much more strategic and agile than their bottom-tier compatriots. In fact, they provision new users, servers, devices and apps **much faster** than the bottom-tier. And, they are **more than twice** as likely to say they focus more on strategic tasks than tactical.

Top-tier performers are not siloed. They prioritize integrated toolsets and teams that collaborate.They also automate basic tasks to improve agility and focus more on providing strategic value, such as ensuring compliance. An IT executive with a provider of cloud-based HR management software says achieving visibility over the network that millions of users access every day has been key to eliminating interdepart-mental road blocks.



"We work so closely with the governance, risk manage-ment, and compliance (GRC) team to ensure that any changes to our IT environment are approved pretty quickly. We are very agile and the job gets done because we need to get the customers what they want in a secure way and as fast as possible."

What can enterprises learn from our top-tier? Five lessons rose to the top:

1

Get Rid of Silos.

Our top-tier respondents reported a high degree of cooperation between network, security and application teams. Only half of the bottom-tier reported that kind of cooperation. With today's highly complex network and application architectures, such cooperation is crucial to allow enterprises to understand network threats and limitations, and to quickly remediate problems. But it is not just siloed teams that impede cooperation. Top-tier organizations were nine times as likely to use integrated security tools, helping to give them a 360-degree view of network and security issues.

2

Pay Attention to Operational Realities.

There is no shortage of security tools for enterprises to choose from. But not all of these are practical to implement or operate. Nearly two-thirds of respondents say IT costs are a somewhat or extremely big challenge. Nearly half say the same of IT staffing. With that in mind, enterprises should choose their network protection tools carefully, making sure the tools they choose won't overtax their staff's time or abilities.

3

Prioritize Based on Risk Analysis.

Network protection is like triage: Nobody has the time or budget to protect against every threat or plug every vulnerability. Your strategy, then, should be to prioritize actions based on a thorough risk analysis. That's one of the reasons the top-tier invests so heavily in security intelligence.

4

Be Realistic about Security Staffing.

Network protection is hard. Increasing network complexity and a fast pace of change guarantee a never-ending stream of security vulnerabilities to address. It takes time – and expertise – to get it right. Be realistic about just how deeply you'll need to staff in security, and in the skills your security professionals need. Our top-tier respondents were 3 times less likely to report being understaffed, one of the factors in their ability to outperform their peers.

5

Automate Routine Tasks.

It is easy to get swallowed-up by the blocking and tackling involved in managing today's complex networks. That leaves your IT organization in a tactical, defensive position. Automating basic tasks (such as provisioning new users) leads to higher IT agility and empowers IT to focus on strategic initiatives. The top-tier are more than three times as likely to automate basic tasks, and are more than twice as likely to report they focus more on strategic issues than tactical.

Infoblox

CONTROL YOUR NETWORK