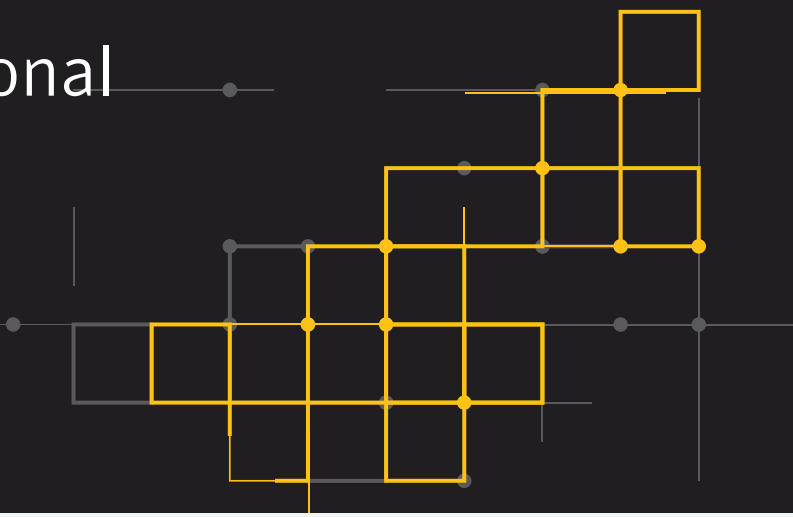
Rackspace Turns Traditional Incident Response into "Proactive Hunting"

Full Packet Capture and Forensics with Security Analytics Drops IR Times from Hours to Minutes



Organization

Rackspace
www.rackspace.com

Industry

Technology – Managed Cloud Services

Challenge

- Accelerate Incident Response processes
- Increase visibility into network threats and attacks
- Move to a more proactive, intelligence-led approach to Incident Response

Solution

Symantec Security Analytics 10g Appliances and Virtual Appliances

Business Benefits

- Slashed IR timeframes from hours to minutes
- Gained actionable insights into all network traffic, including Tor traffic
- Increased the confidence and maturity level of Active Defense team
- Improved customer service and satisfaction levels

For most companies, incident response (IR) costs and timeframes are on an upward spiral. Network-borne attacks are increasingly pervasive, sophisticated, and successful. The question is no longer how to prevent breaches, but how to minimize the time it takes to detect and remediate a breach and get full visibility into what's happening on the network. Rackspace, the #1 managed cloud company, found an answer in Symantec Security Analytics. With Symantec, Rackspace was able to move from reactive IR to proactive hunting of incidents – and in the process cut IR timeframes and costs significantly while improving customer service.

Going proactive: A growing priority

Rackspace helps businesses tap the power of cloud computing by delivering specialized expertise on top of leading technologies developed by AWS, Microsoft, OpenStack, VMware, and others. The company has more than 300,000 customers worldwide, including two-thirds of the Fortune 100, because of its ability to manage complex infrastructure and application platforms. With its growth and success, the company is increasingly dependent on the reliable performance of its internal networks – and avoiding downtime or data loss due to breaches is absolutely critical.

However, the traditional passive model of IR simply wasn't working for Rackspace. Existing IR processes were inefficient and inconsistent; network visibility was limited; and it was impossible to understand the full context of events triggered by its Intrusion Detection System (IDS) and FireEye sandbox.

"We were fighting the same battles every day," said Gary Ruiz, Cyber Security Team Lead, at Rackspace. "We were in passive mode, responding to incidents that occurred with very rudimentary forensic intelligence. Some packet data was available but it wasn't easily accessible. So our IR was sometimes slow and cases were not closed out with a high level of certainty. We needed to move to a more proactive approach to IR."

Rackspace is far from alone in seeing proactive IR as a strategic imperative. In 2015, over 75% of large organizations suffered at least one breach.1 Yet today only 15% of IT professionals feel well-prepared to deal with a security breach,2 only 44% of executives believe that their own enterprise's IR process is either proactive

or mature,3 and just 52% of enterprises have implemented full packet capture and analysis. That is why more sophisticated threat intelligence services are now seen as “must have” network security investments, according to the 2016 Cyberthreat Defense Report.

Full packet capture, full visibility.

A longstanding Symantec customer, Rackspace looked to its trusted partner for a solution to its sluggish IR processes. Symantec recommended a full packet capture solution featuring Security Analytics physical and virtual appliances as a way to proactively gain better visibility, context, and intelligence about network incidents and threats. Now deployed in 12 Rackspace facilities worldwide, the 10G appliances and virtual appliances capture, index, and classify all network traffic in real time – including full packet header and payload – and also provide rapid analysis to support all IR activities.

“With the Security Analytics Appliances we get the insight we need to understand the context of events, so we can contain a breach and remediate immediately,” said Mr. Ruiz. “We get actionable intelligence about threats before, during, and after an attack. That means we can get out in front and get the full source and scope of what’s happening.”

Symantec Security Analytics also provided Rackspace with visibility into its Tor traffic, which is designed to enable anonymous communication and is often exploited by cybercriminals to conceal their location and usage patterns. “Symantec’s DPI engine gives us Tor visibility with high certainty, which adds another layer to our IR capabilities,” said Mr. Ruiz.

Remediation in minutes, not hours

The positive results of moving to proactive IR and full packet capture with the Symantec Security Analytics Appliances are multi-dimensional, according to Mr. Ruiz.

“Originally we wanted the higher visibility of full packet capture so that we could base our IR processes on actual intelligence rather than guesswork,” he said. “We accomplished that and a lot more. Our IR timeframes have dropped in many cases from hours or days to just minutes, and that is saving us a lot in terms of hard-dollar costs and staff time. The quicker you can identify and contain a breach, the less damage is done to the organization and brand.

“Equally important, it is increasing our confidence level,” Mr. Ruiz continued. “Our Active Defense team now knows exactly what’s happening on the network with a high degree of certainty. And that means we spend less time reacting and more time hunting. We can go on mission-specific, intelligence-driven hunting expeditions to root out specific threats and IOCs from sources such as Symantec Intelligence Services, Crowdstrike, third-party forums, FireEye, and so on. We can take whatever action is called for – proactively.”

In addition, Mr. Ruiz mentioned that the support Rackspace has received from Symantec has helped stoke the success with proactive IR. “Symantec support is what we use to benchmark other suppliers,” he said. “They’re proactive in their own right – always there to answer questions and offer solid advice.”

The future favors proactive IR

Looking ahead, Mr. Ruiz said that Rackspace will continue to expand its deployments of Security Analytics because it has proven its value. At the same time, he expressed the view that Symantec has underscored its reputation as a trusted advisor.

“We will continue to turn to Symantec for leading-edge cybersecurity solutions because Symantec has consistently kept us a step ahead in this ongoing arms race,” he said. “With the service and solutions Symantec delivers to us, we can deliver a higher level of service to our customers.”

[1] Source: 2016 Cyberthreat Defense Report, from CyberEdge Group.
[2] Source: CIO Insight, “Most IT Pros Ill-Prepared to Deal With Breaches”
[3] Source: Ponemon Institute, 2015.

About Symantec

Symantec Corporation World Headquarters
350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

SYMC_cs_Rackspace_SA_EN_v1a