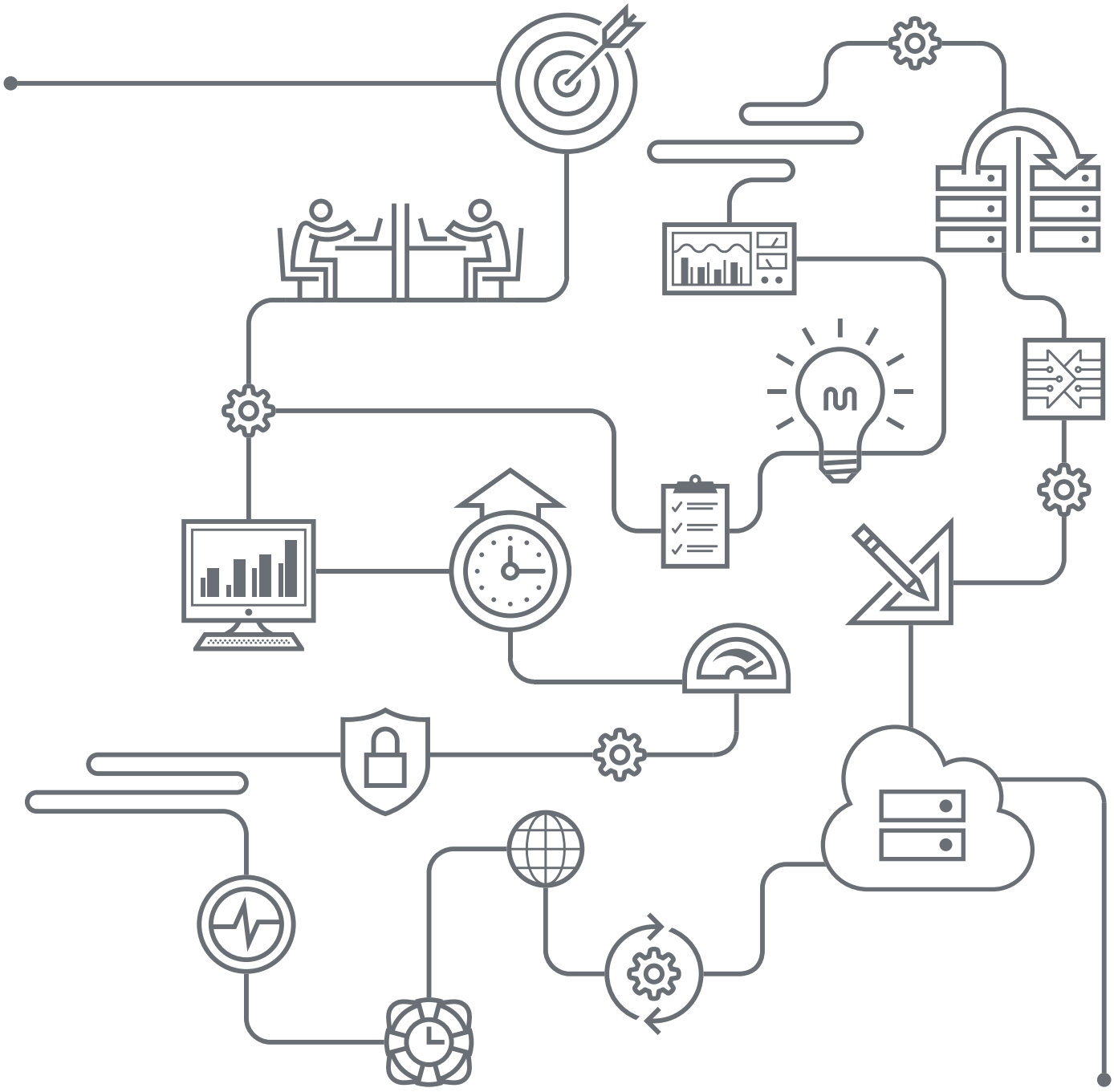
A NEW WORLD, A NEW SECURITY APPROACH

CYBER OPERATIONS FOR THE NEW NORMAL



A NEW SECURITY PARADIGM

A decade ago, the internet completely reshaped the strategies and tools used by technology leaders to protect their data and defend their businesses. Similarly, the more recent explosion of cloud computing services, mobile devices and other new technologies has upended existing security paradigms.

Gone are the days of setting and forgetting the latest tools. New, sophisticated technologies and techniques have enabled our adversaries — be they advanced and persistent or simply malicious and determined — to pick the locks securing our perimeters. Again and again, attackers manage to find a way into enterprise environments. The sheer number of breaches of large, well-resourced companies and government organizations speaks for itself.

And the business risk of breaches continues to rise. According to Forbes, some recent estimates put the annual cost of cyber crime at $500 billion or more — a number that quadrupled from 2013 to 2015 and is expected to do so again by 2019.

These costs closely correspond to the amount of time it takes to discover a breach. Estimates vary, but several recent studies found the average discovery time to be between 150 and 200 days — and many breaches go undetected for years. This can be a difficult reality to digest, but understanding and accepting it will enable security teams to build better strategies for protecting businesses against sophisticated adversaries.

Today's security programs apply innovative new technologies, but they cannot guarantee that a network won't be compromised. The real challenge is to understand the threat, implement controls and capabilities that protect the data and effectively manage the risk. The concept of "business risk proposition" is well known to business leaders worldwide, and it accurately represents the challenge facing today's security leaders, who can no longer afford to see security as only an IT issue.

A NEW APPROACH

To address these new realities, Rackspace Managed Security has built a security operation that incorporates the most effective elements of traditional security strategies while focusing on three key areas that make it uniquely effective in today's threat landscape:

1. We prioritize your data and understand its value to the business.

Yesterday's defensive strategies focused on the perimeter. Today, we are laser focused on data. Rackspace takes a dynamic and contextualized approach to security, rooted in a deep understanding of the data we are protecting and its impact on your business. That understanding points us to the users, systems and data streams that normally interact with your data. With a clear, well-informed picture of "normal," we can tune our tooling and focus our threat intelligence, enabling our cyber hunters to search actively for anything "anomalous."

2. We've abandoned the traditional reactive posture triggered by alerts.

Today, we begin with the assumption that attackers have gained access to a network, and our security operations team proactively hunts them down. When we accept that traditional

perimeter tooling is unlikely to be effective against advanced attackers, we must also accept that adversaries may be active on our networks. This is not an admission of failure. It merely defines the battleground on which we will detect and defeat the enemy.

Fortunately for us, that battle will be fought on home turf. Cyber hunting missions are designed to identify artifacts and activity which, in isolation, appear benign, but in aggregate may indicate an attacker's presence on a network. Using intelligence to break down an attacker's tactics, techniques and procedures (TTPs), we can determine exactly what to look for at a granular level. Highly skilled and experienced cyber analysts can then systematically patrol the environment for any evidence that an attacker has been active, which dramatically accelerates detection.

3. We take immediate action to protect data and minimize business impact.

Too many security operations still employ a reactive monitor-detect strategy. This overreliance on technology to provide an alert, and the resulting graduated response, has helped lead to a crippling average time-to-detect of 150 to 200 days. Detection, when it finally happens, is too far down the kill chain, and the resulting impact on the business is often devastating.

Rackspace Managed Security uses a catalog of preapproved actions to enable a posture of immediate response. We understand our environment, priorities and arsenal of security tools far better than any attacker could. We use this advantage ahead of time to plan, validate and approve the actions we must take to be effective when we identify malicious activity. Starved of time, an attacker is much less likely to identify the data he seeks or achieve a persistent presence in the environment.

CONCLUSION

Delivering a robust and effective security operation in today's threat landscape is no trivial task, and a shift in thinking is a critical first step. To effectively manage business risk, security practitioners must become security leaders — capable not only of building complex security operations and leading the daily fight against attackers, but also of guiding their business units and boardrooms through an increasingly complex decision-making process.

Detecting and responding effectively to today's attackers means putting the data you are protecting at the heart of your security operation, adopting a proactive approach to detecting anomalous activity on your network, and honing your ability to respond swiftly and effectively to malicious activity when it is detected.

Dangerous and sophisticated attacks are a daily challenge for security teams everywhere. This is the new normal. An effective security strategy must deploy highly skilled analysts to actively patrol networks, guided by a thorough understanding of the data they are protecting and its importance to the business. And those analysts must be agile enough to respond immediately.

Such an operation will make our adversaries' work more complex, more expensive and more likely to fail.

ABOUT RACKSPACE

Rackspace (NYSE: RAX), the No. 1 managed cloud company, helps businesses tap the power of cloud computing without the challenge and expense of managing complex IT infrastructure and application platforms on their own. Rackspace engineers deliver specialized expertise on top of leading technologies developed by OpenStack®, Microsoft®, VMware® and others through a results-obsessed service known as Fanatical Support®.

Learn more at www.rackspace.com/**managed-security**, or call us at **1-800-961-2888**.

rackspace®

Learn more at www.**rackspace**.com/**managed-security**