ABOUT RAPID7 - OUR STORY

Overview

Rapid7 is a leading cyber security solutions provider, on a mission to make successful security tools and practices accessible to all. Rapid7 Insight Platform technology, expert services, and thought-leading research enables over 9,000 customers to improve their security programs so that they can safely advance and innovate.

In the nearly 20 years that Rapid7 has been in business, security companies and trends have come and gone, while broader technology innovation continues to advance rapidly. Every company is now a technology company, and rampant innovation inevitably creates security risk. The migration of businesses to the cloud and ubiquitous connected devices present security teams with an increasingly complex, ever-changing, and unpredictable attack surface.

We believe as cybersecurity challenges continue to rise exponentially, two key factors can prevent organizations from effectively managing their growing security exposure. First, the tools to manage complex security problems are often complicated to use. Second, there is a scarcity of cybersecurity professionals who are qualified to successfully manage these sophisticated tools. These two factors compound the difficulties that resource-constrained organizations face when attempting to minimize their security exposure, meet security compliance regulations and provide visibility to their leadership. The expanding divide between risk created through innovation and risk managed by security teams is called the Security Achievement Gap.

We believe Rapid7 is uniquely positioned to improve how customer security challenges are addressed. Our solutions simplify the complex, allowing teams to more effectively reduce vulnerabilities, monitor malicious behavior, investigate and shut down attacks, and automate routine tasks. All of our solutions and services are built with and supported by the expertise of our dedicated team of security researchers and consultants, who bring knowledge of attacker behavior and emerging vulnerabilities directly to customers. We also continue to invest in further simplifying our technology to improve usability, lowering the barrier to managing security for teams and organizations who lack resources.

While our security technology is the foundation of our mission to make successful security accessible to all, technology alone will not solve today's cybersecurity challenges. Our ongoing commitment to researching and partnering with the technology community helps to curb new security risks born through innovation. We are also investing in under-served, at risk communities, like non-profits and hospitals, to better understand their needs and make security technology and services accessible.

By continuously improving our technology, stemming the creation of risk in the community, and making security more usable and accessible, Rapid7 aims to close the Security Achievement Gap. As of December 31, 2019, we had more than 9,000 customers that rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations.

Our Solutions

We offer products across the four main pillars of on our Insight Platform:

• **Vulnerability Risk Management:** Our industry-leading Vulnerability Risk Management (VRM) solutions provide clarity into risk across traditional and modern IT environments, and the capabilities and data to influence remediation teams and track progress. With built-in risk prioritization, IT-integrated remediation projects, tracking of goals and service level agreements, and pre-built automation workflows, our solutions are designed to not just enumerate risk, but also accelerate risk mitigation.

• **Incident Detection and Response:** Our Incident Detection and Response (IDR) solutions are designed to enable organizations to rapidly detect and respond to cyber security incidents and breaches across physical, virtual and cloud assets. Equipped with user behavior analytics (UBA), attacker behavior analytics (ABA), end-point detection and response (EDR) and deception technology, our Security Information and Event Management (SIEM) is designed to provide comprehensive network visibility and accelerate threat investigation and response.

• **Application Security:** Our Application Security offerings provide dynamic application security testing and run-time application security monitoring and protection solutions that are designed to continuously analyze web applications for security vulnerabilities throughout a customer's software development life cycle.

• **Security Orchestration and Automation Response:** Our Security Orchestration and Automation Response (SOAR) solutions allow security teams to connect disparate solutions within their cyber security, IT and development operations and build automated workflows, without requiring code, to eliminate repetitive, manual and labor-intensive tasks, resulting in measurable time and cost savings.

Finally, to complement our products, we offer a range of managed services based on our software solutions and professional services, including incident response services, security advisory services, and deployment and training.

Insight Platform

Our cloud-native Insight Platform is at the core of our product offerings. The platform was built using our extensive experience in collecting and analyzing data to enable our customers to create and manage analytics-driven cyber security risk management programs. By utilizing our powerful, proprietary analytics to assess and understand the context and relationships around users, IT assets and cyber threats within a customer's environment, our solutions make it easier for teams to manage vulnerabilities, monitor for malicious behavior, investigate and shutdown attacks, and automate operations.

Our Insight Platform provides a high level of scalability. We leverage on-premise deployment models and cloud technologies to achieve a scalable delivery model with a high degree of redundancy, fault tolerance, and cost-effectiveness.

We also designed our Insight Platform to provide a secure environment for our customers data. We deploy a variety of technologies and practices that are designed to help ensure that the data collected from a customer's environment remains proprietary, secure and operational.

Insight Platform's Features:

Visibility:

The Insight Platform allows security professionals to collect data once across their IT environment, enabling Security, IT, and development operations (DevOps) teams to collaborate effectively as they analyze shared data.

• Unified Data Collection:

We designed the Insight Platform to allow customers to collect their data once and leverage that same data across multiple solutions, providing shared visibility across teams and reducing time to value for additional solutions. Our robust data collection architecture supports gathering a wide swath of operational data from endpoints to the cloud, including key data about assets and user-specific behavior, into a unified, searchable dataset.

• Agentless and Agent-Based Architecture:

We developed our platform with flexible processing technologies that employ both agentless data collection and our own internally-developed endpoint agent technology, which enables rapid and seamless integration of our products into our customers' modern IT environments and provides security and IT professionals with instant visibility into their dynamic and rapidly-expanding IT ecosystem. Our lightweight endpoint agents are designed to automatically collect data from all endpoints, even those from remote workers and sensitive assets that cannot be actively scanned, or that rarely join the corporate network.

• Endpoint Detection and Visibility:

With a universal lightweight agent and endpoint scanning, the Insight Platform provides real-time detection and the ability to proactively remediate IT environments, before a potential attack happens.

• Cloud and Virtual Infrastructure Assessment:

Modern networks and infrastructures are constantly changing. The Insight Platform integrates with cloud services and virtual infrastructure to help ensure that technology is configured securely and that security professionals know when new devices are brought online.

• Attack Surface Monitoring with Project Sonar:

As organizations grow and infrastructure becomes more complex, maintaining visibility into attack surface becomes more challenging.

Our platform directly integrates with Project Sonar, a Rapid7 research project that regularly scans the public internet, to gain insights into global exposure to common vulnerabilities. This capability also enables security professionals to identify previously unknown, externally facing assets connected to the internet.

Analytics:

Increasing IT environment complexity coupled with a severe lack of cyber security professionals is overwhelming security and IT teams, who are struggling to deal with false positives and maintain adequate levels of cyber security. Our Insight Platform addresses these challenges with the following features:

• User and Attacker Behavior Analytics:
Our Insight Platform incorporates extensive user behavior analytics (UBA) and attacker behavior analytics (ABA) to provide rapid context around users, attackers and assets involved in an incident, enabling organizations to more quickly respond to, contain and mitigate breaches. Our platform incorporates comprehensive UBA to create a behavior profile for each user and correlates every event with a user, asset or application to detect compromised credentials, lateral movement and other malicious behavior.

• Risk Prioritization and Management:
With built-in risk assessment and risk prioritization, IT-integrated remediation projects, and pre-built automation workflows, the Insight platform provides a granular view of what is relevant and critical today, to help ensure risks can be prioritized and mitigated more effectively.

• Threat Detection:
Our Insight Platform includes integrated threat feeds, informed by public data as well as proprietary threat intelligence and adversary research, and continuously gathers and combines them with a customer's IT environment, to show threats that are most relevant to them. • Centralized Log Management: Our cloud-based platform correlates millions of daily events in any IT environment directly to the users and assets behind them to highlight risk across the environment and help prioritize where to search and automate compliance without the requirement of extensive hardware.

• Deception Technology:

Monitoring solutions that only analyze log files leave traces of the attacker unfound. Through our deep understanding of attacker behavior, our Insight Platform provides not only UBA and endpoint detection, but also easy-to-deploy intruder traps. These include honeypots, honey users, honey credentials, and honey files, all crafted to identify malicious behavior earlier in the attack chain.

• Industry Experts:

With a highly specialized team of penetration testing, incident response, threat hunting and security operation center experts, we believe we are uniquely positioned to stay ahead of emerging threats and help detect threats quickly across a customer's entire IT ecosystem.

Automation:

Our Insight Platform unites technology stack and allows security operations teams to connect disparate solutions within their cyber security, IT and development operations.

• Built-in Workflows:

Security tools have not historically been built to work well together, and without deep programming knowledge, building automation between tools was nearly impossible. With our Insight Platform, security professionals can streamline their operations with connect-and-go workflows, without requiring any code, resulting in significant time and cost savings. Examples of these workflows include assisted patching and automated containment.

• Highly Customizable:

The Insight Platform not only has a wide range of pre-built workflows and integrations, it is also highly extensible. With approximately 300 plugins to connect security tools and easily customizable connect-and-go workflows, the Insight Platform frees up security teams to tackle other challenges, while still leveraging human decision points when it is most critical.

Insight Platform Product Offerings

We offer our Insight Platform solutions as software-as-a-service products, on a subscription basis. Our Insight Platform products are available globally and reduce the need for customers to manage large, complex, data infrastructure. We offer the following cloud products across the four main pillars of Security Operations (SecOps):

InsightVM:

Utilizing the power of our Insight Platform, InsightVM is designed to provide a fully available, scalable, and efficient way to collect vulnerability data, prioritize risk and automate remediation.

InsightVM is designed to provide prioritized guidance based on customized threat models; dynamic live dashboards that are easily customizable and queried; lightweight agents for continuous visibility; integration with cloud services, virtual infrastructure and container repositories such as dockers; in-product integration with solutions such as ServiceNow, IBM Bigfix, Microsoft SCCM and Jira ticketing systems; and remediation workflow for assigning and tracking remediation progress within the product. Embedded workflows also allow Security and IT teams to automatically deploy compensating controls for vulnerabilities that cannot be patched.

InsightVM is offered through a cloud-based subscription or as a managed service. The managed service is known as Managed Vulnerability Risk Management, which provides our resource constrained customers with a fully outsourced option for leveraging our innovation, expertise and technology.

InsightIDR:

InsightIDR, our Incident Detection and Response (IDR) solution, is designed to enable organizations to rapidly detect and respond to cyber security incidents and breaches across physical, virtual and cloud assets.

InsightIDR unifies SIEM, UBA, and endpoint detection to detect stealthy attacks across today's complex networks. It analyzes the billions of events that occur daily in organizations to reduce them to the important behaviors and deliver high-fidelity and prioritized alerts. In addition to identifying stealthy attacks often missed by other solutions, InsightIDR focuses the security team on issues that warrant investigation and reduces the time to investigate with its user correlation, powerful search and endpoint interrogation capabilities.

InsightIDR is designed to provide a cost-effective response to the need for SIEM. With our Metasploit community, research and incident response services, we are continually studying and identifying the latest attacker methods. We have found ways to increase accuracy, speed

processes, and achieve greater confidence, even as attacker methods change. These include built-in deception capabilities such as honeypots and automated threat intelligence feeds that quickly alert our customers to new attacker behaviors seen in the wild by our own threat hunters.

Unlike most SIEMs, InsightIDR also provides the capability to seamlessly act on many threats automatically, thus further reducing the time from detection to response. InsightIDR includes out-of-the-box automation workflows to improve analyst productivity such as automated containment to mitigate an attack. Additionally, with the Insight Agent, users can kill malicious processes or quarantine infected endpoints from the network. They can also use InsightIDR to take containment actions across Active Directory, Access Management, EDR, and firewall tools.

InsightIDR is offered through a cloud-based subscription or as a managed service. The managed service is known as Managed Detection and Response, a fully outsourced service that combines our team of expert analysts with InsightIDR. When attacks are found, customers are promptly informed of all known details and our team moves to incident response, providing security teams with detailed, easy-to-follow remediation steps tailored to the environment.

InsightAppSec:

InsightAppSec provides comprehensive dynamic application security testing that continuously analyzes web applications for security vulnerabilities.

The key features include: a universal translator to enable IT security professionals to analyze complex applications; customized attack simulation capabilities that allow automatic testing of workflows such as shopping carts; scanning automation; attack replay, which allows replay of vulnerabilities in real time in order to verify that vulnerabilities are exploitable and that successful remediation has occurred; continuous site monitoring, which detects changes in application ecosystems and triggers a re-scan according to configurable settings; and integration with ticketing systems.

InsightAppSec enables integration with protection technologies to automatically generate web application firewalls (WAFs), which are custom rules that help to protect vulnerable applications while the vulnerabilities are being remediated.

InsightAppSec supports most leading WAFs, including F5, Sourcefire and Imperva. InsightAppSec is offered on a cloud-based subscription basis or as a managed service. The managed service is known as Managed Application Security and provides a fully outsourced option for application scanning and security testing.

InsightConnect:
InsightConnect is our SOAR solution that is used by security professionals to connect their many disparate solutions and automate workflows to increase the speed with which they can identify risk and respond to incidents. With a growing library of approximately 300 plugins to connect tools and easily customizable connect-and-go workflows, it allows our customers to automate manual and tedious tasks, while still leveraging their expertise when it is most critical, thereby saving time and improving efficiency. InsightConnect is offered on a cloud-based subscription basis.

Other Products

Nexpose: Nexpose is an on-premise version of our Vulnerability Risk Management solution, that enables customers to assess and remediate their overall exposure to cyber risk across their increasingly complex IT environments. Nexpose is offered through term-based software licenses.

AppSpider: AppSpider is the on-premise version of our Application Security Testing solution that provides comprehensive dynamic application security testing that continuously analyzes web applications for security vulnerabilities. AppSpider is offered through term-based software licenses.

Metasploit: Metasploit is an industry-leading penetration testing software solution, developed on an open source framework. Metasploit can be used to safely simulate attacks on an organization's network in order to uncover vulnerabilities before they are exploited by cyber attackers and assess the effectiveness of an organization's existing defenses, security controls and mitigation efforts. The Metasploit open source framework is freely available and geared toward developers and security 5 researchers. We also offer Metasploit Pro, the commercial penetration testing software based on the Metasploit framework, through term-based software licenses.

InsightOps: InsightOps simplifies IT infrastructure monitoring and troubleshooting by centralizing data from across a customer's network into one secure location. With scalable and cost-effective architecture and the ability to bring together asset visibility and log management,

InsightOps enables organizations to store and search structured, semi-structured and unstructured data in real time, enabling DevOps and IT professionals to centralize, search and monitor their log data in order to investigate anomalies, troubleshoot issues and conduct root cause analysis.

Professional Services

Our professional services offerings enhance our ability to serve as a trusted advisor in assisting organizations to think proactively about their security programs and implement strategic, analytics-driven security strategies. We believe that our role as trusted advisor helps drive better security outcomes for our customers, as well as loyalty and further usage of our products. Our professional services offerings include, but are not limited to, Penetration Testing, Cyber Security Maturity Assessments, Security & Incident Response Program Development Services, IoT & Internet Embedded Device testing as well as Threat Modeling, TableTop Exercises and Incident Response services. In addition, we offer deployment and training services related to our platform, to further help customers operationalize and customize their platform experience. For example, our Cyber Security Maturity Assessments provide our customers with a view of their current security posture, an objective review of their existing plans, and a guide to their strategic planning. By accessing our security talent, we help organizations develop an approach and road map to further mature and strengthen their program efforts - often simplifying the otherwise complex.

Research and Development Efforts

We invest substantial resources in research and development to enhance our core technology platform and products, develop new end market-specific solutions and applications, and conduct product and quality assurance testing. Our technical and engineering team monitors and tests our products on a regular basis, and we maintain a regular release process to refine, update, and enhance our existing products. We also have a team of experienced security researchers who work to keep us abreast of the latest developments in the cyber security landscape. Our research and development teams are located in our offices in Boston, Massachusetts; Austin, Texas; Los Angeles and San Francisco, California; Arlington, Virginia; Toronto, Canada; Dublin and Galway, Ireland; Belfast, Northern Ireland; and Stockholm, Sweden, providing us with a broad, worldwide reach to engineering talent.

Metasploit Community:
Our Metasploit product has an active community of contributors and users. This online security community provides us with a robust and

growing network of active users and influencers who promote the usage of our software. Security researchers contribute modules to the Metasploit Framework that serve as a resource about real-world attacker techniques. The community also provides us with near real-time visibility into new cyber attacks as they occur and a deep understanding of attacker behaviors. We perform security research that enables the analytics in our platform and products as well as delivers strategic value to the security community at large.

The output of our research results in threat intelligence, exposure analysis and attacker awareness that we publish as well as integrate into our platform. This data is used for security research, product development, and across our services to help protect and inform our customers, partners and community. We share this data with validated educational and private security researchers, research partners, vetted threat sharing communities, and organizational security teams through our Open Data portal to foster collaboration and encourage discovery of new insights. We collect data for research purposes through two key areas:

Attacker Intelligence: We collect data from across the internet through a variety of honeypots distributed both geographically and across IP space. The honeypots collect many data types which are then analyzed to help enhance our understanding of attacker methods.

Internet Intelligence: We conduct internet-wide scans across many services and protocols to gain insight into global exposures and vulnerabilities. This data collected is analyzed for the purpose of analytics in our platform and results in core research reports. We publish a variety of reports including The National Exposure Index, The Industry Cyber Exposure Report and Under the Hoodie. The 7 National Exposure Index, published annually, is a census report that highlights the state of exposed internet services at the nation-state level and provides key trending information on the use of insecure protocols. The Industry Cyber Exposure Index details the attack surface, insecure service presence, email safety configurations, malware infection rates and internet supply chain risks of Fortune 500 companies. The Under the Hoodie report sheds light on the art of penetration testing by revealing not just the process, techniques and tools that go into it, but also revealing the real-world experience of our engineers and investigators, gathered over thousands of penetration tests.

Our Customers

Our customer base has grown from approximately 5,100 customers at the end of 2015 to more than 9,000 customers as of December 31, 2019, in 144 countries, including 47% of the organizations in the Fortune 100. In 2019, 52% of our revenue was generated from large enterprises, which we define as organizations that have either annual revenue greater than $1.0 billion or more than 2,500 employees, and the balance was generated from middle-market and small organizations. Our revenue is not concentrated with any individual customer and no customer represented more than 1% of our revenue in 2019, 2018 or 2017.

Our Competition

The markets we operate in are highly competitive, fragmented and subject to technology change and innovation. Our primary competitors in Vulnerability Risk Management include Qualys and Tenable; in Incident Detection and Response (SIEM) include Splunk, Micro Focus and LogRhythm; in Application Security include Micro Focus and IBM; in Security Orchestration and Automation Response include Phantom (Splunk) and Demisto (Palo Alto Networks); and finally, while the competition in our professional services business is diverse, our competitors include FireEye's Mandiant, SecureWorks and NCC Group.

We compete on the basis of a number of factors, including: • product functionality; • breadth of offerings; • performance; • brand name, reputation and customer satisfaction; • ease of implementation, use and maintenance; • total cost of ownership; and • scalability, reliability and security. Some of our competitors have greater sales, marketing and financial resources, more extensive geographic presence or greater brand awareness than we do. We may face future competition in our markets from other large, established companies, as well as from emerging companies. In addition, we expect that there is likely to be continued consolidation in our industry that could lead to increased price competition and other forms of competition.

Intellectual Property

Our future success and competitive position depends in part on our ability to protect our intellectual property and proprietary technologies. To safeguard these rights, we rely on a combination of patents, trademarks, copyrights, trade secrets, employee and third-party nondisclosure agreements, licensing arrangements and other contractual protections to protect our intellectual property in the United States and other jurisdictions. We have numerous issued patents and a number of registered and unregistered trademarks. We believe that the duration of our issued patents is sufficient when considering the expected lives of our products. We file patent applications to protect our intellectual property

and have a number of patent applications pending. We require our employees, consultants and other third 8 parties to enter into confidentiality and proprietary rights agreements and control access to software, documentation and other proprietary information. Although we rely on intellectual property rights, including trade secrets, patents, copyrights and trademarks, as well as contractual protections to establish and protect our proprietary rights, we believe that factors such as the technological and creative skills of our personnel, creation of new modules, features and functionality, and frequent enhancements to our solutions are more essential to establishing and maintaining our technology leadership position.

We also license software from third parties for integration into our offerings, including open source software and other software available on commercially reasonable terms. We believe our continuing research and product development are not materially dependent on any single license or other agreement with a third party relating to the development of our products.

Employees

As of December 31, 2019, we had 1,544 full-time employees, including 294 in product and service delivery and support, 656 in sales and marketing, 393 in research and development and 201 in general and administrative. As of December 31, 2019, we had 1,118 full-time employees in the United States and 426 full-time employees internationally.

Corporate Information

We were initially incorporated in July 2000 in Delaware. Rapid7 LLC, a limited liability company organized under the laws of the Commonwealth of Massachusetts, was formed in January 2004. In August 2004, pursuant to an exchange agreement among Rapid7 LLC and the stockholders of Rapid7, Inc., the stockholders exchanged their shares in Rapid7, Inc. for equity interests in Rapid7 LLC, after which Rapid7, Inc. was dissolved. In August 2008, Rapid7 LLC was merged with and into Rapid7 LLC, a newly-formed Delaware limited liability company. Rapid7, Inc. was reincorporated in Delaware in October 2011. In a series of transactions in November 2011, equity holders of Rapid7 LLC exchanged their equity interests in Rapid7 LLC for capital stock in Rapid7, Inc. and Rapid7 LLC became a wholly-owned subsidiary of Rapid7, Inc.

Our principal executive offices are located at 120 Causeway Street, Boston, Massachusetts.

Our telephone number is +1 617-247-1717.

Our website address is www.rapid7.com.