1H 2019
Vulnerability and Exploit Trends

presented by eSentire Managed Vulnerability Service

eSENTIRE®

PREFACE

The following is a summary of vulnerability trends observed and investigated by the eSentire Security Operations Center (SOC) in 1H 2019.

To help customers stay on top of the expanding vulnerability landscape, eSentire delivers Managed Vulnerability Service. A team of dedicated experts work with over 140 clients globally to streamline their vulnerability and patch management programs, shrink the time to remediate damaging vulnerabilities and reduce overall cyber risk.

eSentire's Managed Vulnerability Service is a comprehensive vulnerability management solution that combines cutting-edge technology with the security expertise of the industry's leading Managed Detection and Response (MDR) provider.

THREAT ACTORS ARE CAPITALIZING ON THE GROWING NUMBER OF VULNERABILITIES WITH INCREASING SPEED.

The graph in Figure 1 visualizes the challenge all organizations face when it comes to vulnerability management. Situated right at the point where the two graph lines intersect, most security teams are being squeezed by a vice grip of an increasing number of vulnerabilities and the velocity at which threat actors are operating.

VULNERABILITY WEAPONIZATION TIME

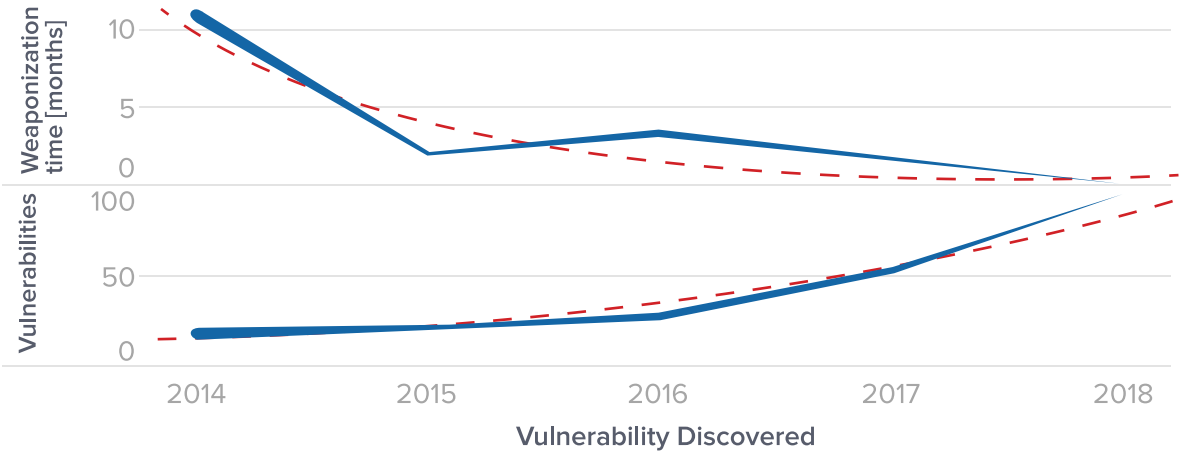


Figure 1: *eSentire Q1 2019 quarterly threat report*

A majority of organizations are reporting insufficient vulnerability management resources and cumbersome processes, adding to the challenge posed by the threat landscape.

58%

say they have inadequate staffing to scan vulnerabilities in a timely manner

51%

spend more time navigating manual processes than responding to vulnerabilities, leading to insurmountable response backlogs

48%

say their organization is at a disadvantage in responding to vulnerabilities because they use manual processes

Ponemon Institute LLC: Measuring & Managing Cyber Risks to Business Operations: December 2018

THE MOST VULNERABLE INDUSTRIES

Insurance, followed by technology and finance are the most vulnerable industry verticals as observed by eSentire's Security Operations Center (SOC).

When observing this data It is worth mentioning the obvious: all it takes is one vulnerable endpoint for a threat actor to exploit and breach a network. An organization could have just one of 10,000 endpoints (or 0.001%) unpatched and vulnerable and be compromised in the same way as the insurance, technology and finance industries that have more than 10 percent of endpoints with vulnerabilities. Maintaining an effective vulnerability management program that consistently keeps the number of vulnerable endpoints as close to zero as possible greatly reduces overall cyber risk.

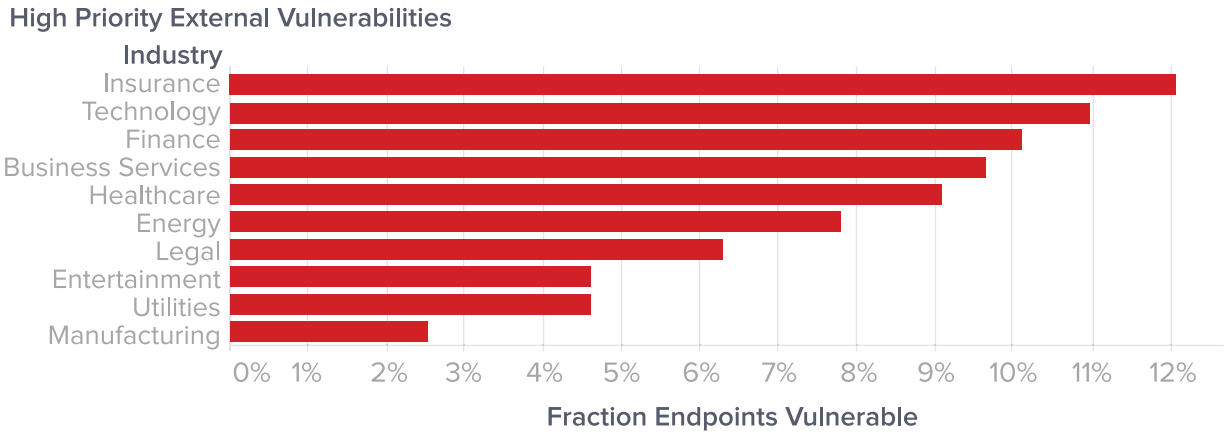
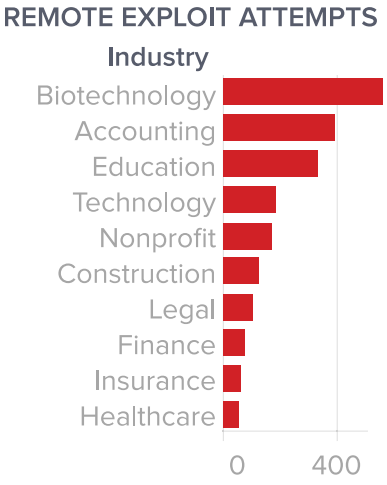


Figure 2: *eSentire SOC Data Q1 2019*
Note: This data is a reflection of eSentire's customer total customer base, not specifically Managed Vulnerability Service customers.

THE MOST TARGETED INDUSTRIES

Biotechnology followed by accounting and education are the industries observed to be the most targeted by threat actors looking to leverage exploitable vulnerabilities.



There are some possible explanations for this data. In the case of the accounting industry, Q1 is by far the busiest time of year with income tax season in the United States, Canada and the United Kingdom. The increased volume of sensitive financial data exchanging hands makes an attractive target for threat actors.

Figure 3: *eSentire SOC Data Q1 2019. Note: This data is a reflection of eSentire's customer total customer base, not specifically Managed Vulnerability Service customers.*

PREDICTING THE PROBABILITY OF BREACH DUE TO EXPLOITATION

eSentire used SOC data reflective of 650 organizations spread over more than 50 countries. The data was used to determine future probabilities contextual to the number of locations protected and the industry in which an organization operates. Propensity modeling produced cumulative probabilities of at least one incident that would bypass an organization's existing controls over a calendar year. The chart below features data specific to exploitation.

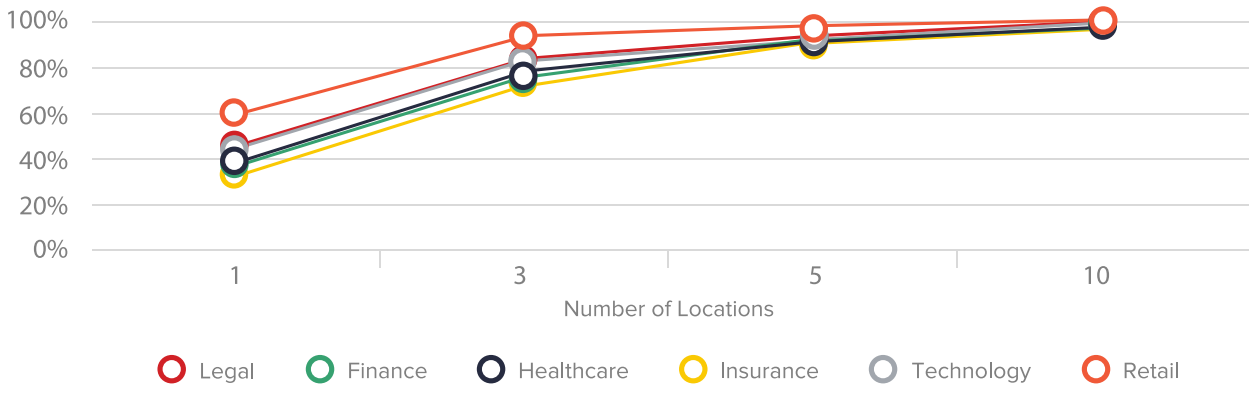


Figure 4: *Compounded risk of an incident due to exploitation by industry*
Note: This data is a reflection of eSentire's customer total customer base, not specifically Managed Vulnerability Service customers.

THE ESENTIRE MANAGED VULNERABILITY SERVICE DIFFERENCE

eSentire Managed Vulnerability Service positions IT security teams to stay on top of the increasingly challenging vulnerability landscape.

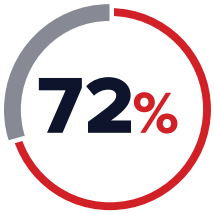
Powered by the industry's leading vulnerability management platform, scanning is available for more than 109,000 known vulnerabilities across a variety of IT assets including web applications, mobile devices, IoT devices and cloud environments.

> We have increased visibility into what is going on inside and outside our environment than we ever had before.
>
> — IT Manager, medium enterprise wholesale distribution company and Managed Vulnerability Service customer

eSentire's dedicated Managed Vulnerability Service team works with customers throughout the vulnerability management lifecycle, facilitating timely and accurate scanning, remediation guidance and comprehensive reporting.

These ongoing activities enable customers to shrink the critical vulnerability discovery-to-remediation timeframe that attackers look to capitalize on. Additionally, valuable time and resources are freed up to allocate to other IT security priorities.

of eSentire Managed Vulnerability Service clients have reported an **overall improvement** in their security posture



of eSentire Managed Vulnerability Service customers experienced a **reduction in time to detect threats**

- eSentire and TechValidate Customer Survey, May 2019

eSentire

eSentire, the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire.**