



Rhetorik Enterprise Technology Insights Report

UK & Ireland Security Software Market
2020

Executive Summary

The UK market for enterprise cyber security solutions is evolving quickly. Our analysis of that demand – as reflected by the presence of different security software solutions and the number of potential buyers – shows it to vary considerably by industry vertical and business size.

This report, based on primary research, analysis of Rhetorik's NetFinder™ database and HG Insights, highlights for sales and marketing professionals the key industry sectors and business sizes most likely to have dedicated cybersecurity professionals, those most likely to have Security Software solutions, and how these vary for different types of security software.

1. *Where to focus: Industry Sector Maturity and Opportunity*

Overall, the Public Sector (Education, Government, and Healthcare) and Banking & Finance are much more likely to have **Security Software** solutions, especially compared to the likes of Construction & Contractors and Food & Beverage firms (Figure 5).

These high-presence sectors are also the most likely to be targets of cyber-attacks, according to the National Cyber Security Centre (NCSC) 2019 annual review (page 7).

Yet, while public sector records the highest levels of overall presence of security solutions, it ranks low in Endpoint Security Solutions and Unified Threat Management (ESS/UTM) - one of nine security software technologies tracked in the NetFinder™ platform. (Figure 16).

For ESS/UTM vendors and MSPs looking for new opportunities, public sector appears ripe for growth for new solutions given their relatively low penetration.

2. *Where to focus: Business Size*

SMB shows significant opportunity for new account growth – especially for solutions beyond anti-virus and anti-malware, the first security tools a company might acquire.

Business sites with more than 250 employees are much more likely to already have Security Software applications than sites with fewer employees, while larger enterprises with 1,001 to 2,500 employees on site are the most likely to have already purchased security solutions. These accounts may be targets for more advanced integrated managed solutions (e.g. detection and intervention) as they mature and add new cyber expertise.

3. *Who to target: Cybersecurity Job Functions*

The Banking & Finance sector is 3 times more likely than average to have a dedicated IT Security job function on-site (Figure 8) based on our analysis of more than 180,000 contacts within the NetFinder database. Other sectors that over-index include Services, IT, Retail and Government sectors.

There is also a strong correlation between prevalence and size, with the largest sites more than 4 times more likely than average to have a dedicated IT Security job function on-site (Figure 9).

Contents

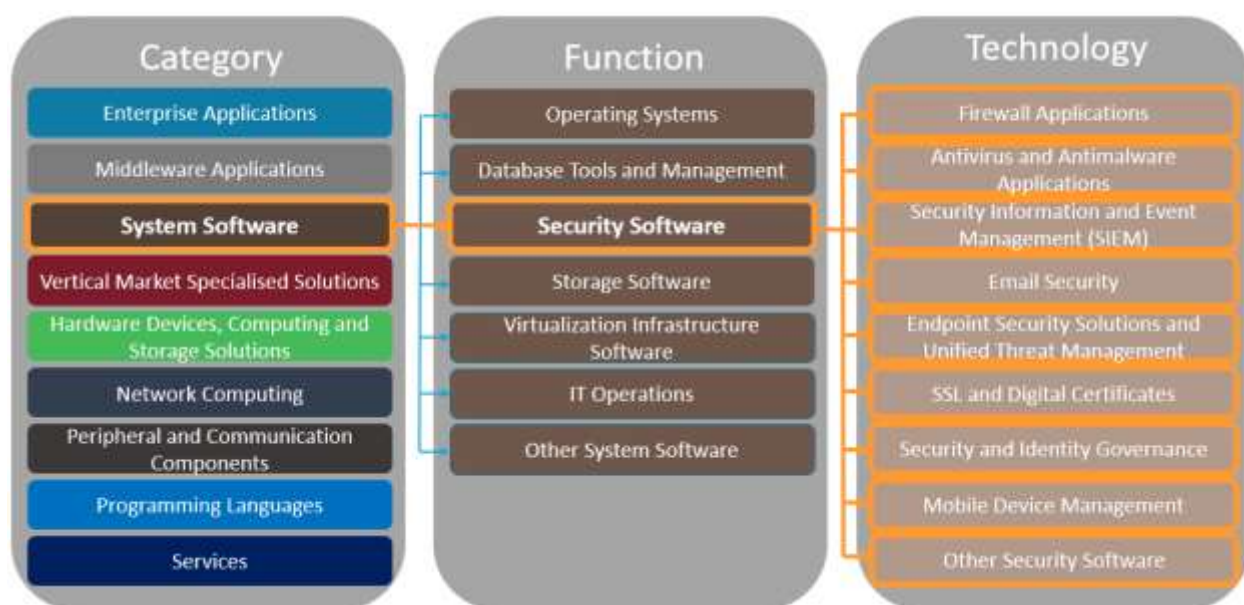
1. Introduction	4
2. NetFinder End-user Organisations Overview	5
3. Security Software Technologies Overview	7
4. Antivirus and Antimalware Applications	11
5. Endpoint Security Solutions and Unified Threat Management	14
6. Security and Identity Governance	17
7. Methodology	20
8. About Rhetorik	21

1. Introduction

Welcome to the new series of Rhetorik Market Reports based on analysis of data available in the NetFinder™ sales and marketing intelligence portal.

This report analyses a range of key “**Security Software**” technologies used within UK and Ireland organisations. The data are drawn from a base of more than 40,000 end-user establishments and the analysis for each category is drawn from a subset of the available data.

Sitting within the System Software “category”, the Security Software “function” comprises 8 separate “technologies” within the proprietary Rhetorik Technology Classification system (see chart below):



A profile of the end-user establishments covered in the report is provided in Section 2, followed by an overview of the data related to **Security Software** in Section 3. This is followed by a more detailed look at three of the nine technologies within the Security Software function – Antivirus & Antimalware Applications (AV/AM – Section 4), Endpoint Security Solutions & Unified Threat Management (ESS/UTM – Section 5), and Security & Identity Governance (SIG – Section 6).

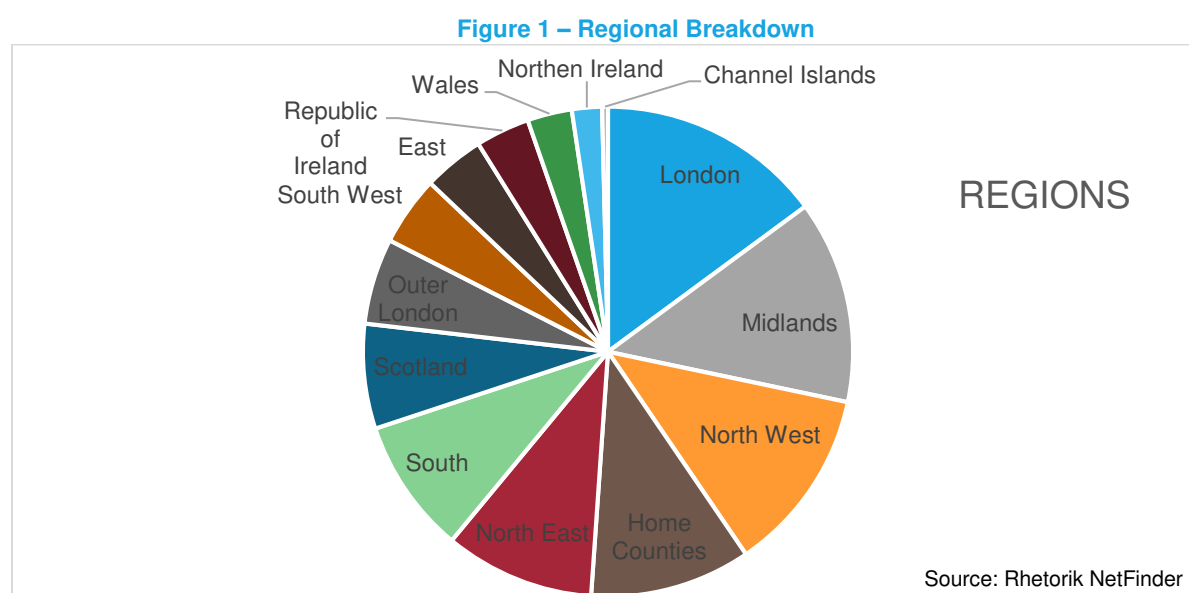
An outline of the research methodology applied in the NetFinder research programme is given at the end of this report (Section 7).

2. Profile of NetFinder End-user Establishments

This chapter provides a summary profile by geographical region and key vertical market sector for sites making up the NetFinder database and used as the basis for top level analysis in this report.

2.1 Profile by Geographic Region

96% of the IT and Telecoms end-user sites analysed are based in the UK, with the remaining 4% in the Republic of Ireland. The regional profile of these user establishments is given in Figure 1.



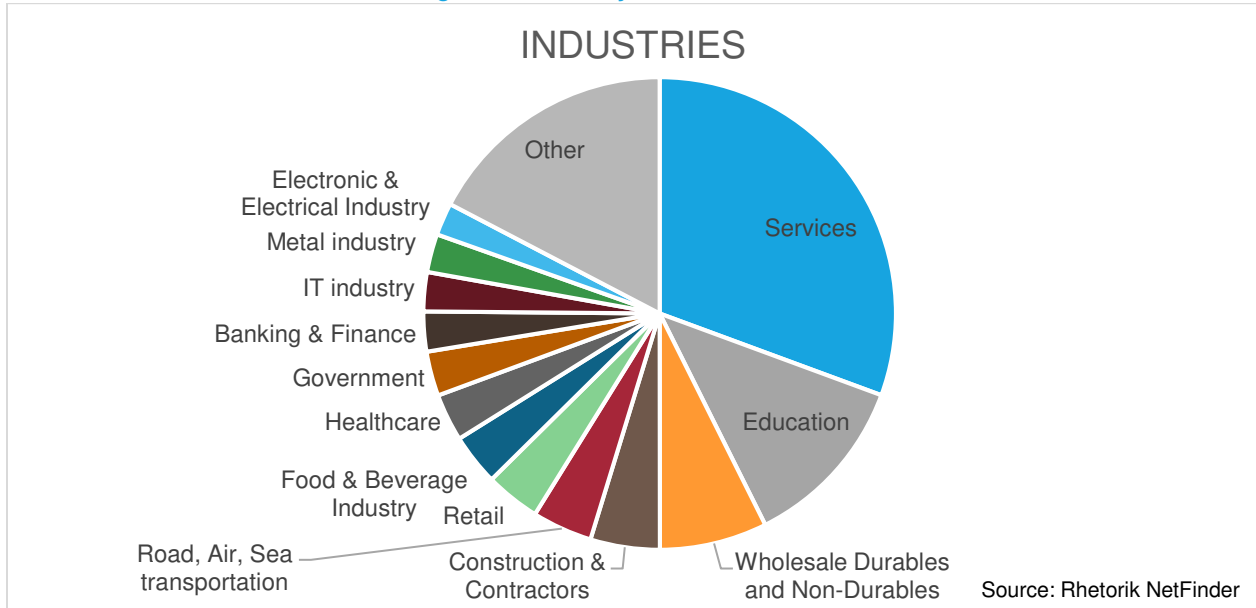
The chart illustrates a broad sample distribution across all regions of the UK. The user-base for these technologies is clearly well-distributed throughout the country.

The 4% of sites based in the Republic of Ireland are mainly concentrated around Dublin and in the South-West of the country.

2.2 Profile by Industry Sector

By industry sector, the enterprise technology end-user base is distributed across all sectors of the economy, as shown in Figure 2.

Figure 2 – Industry Sector Breakdown



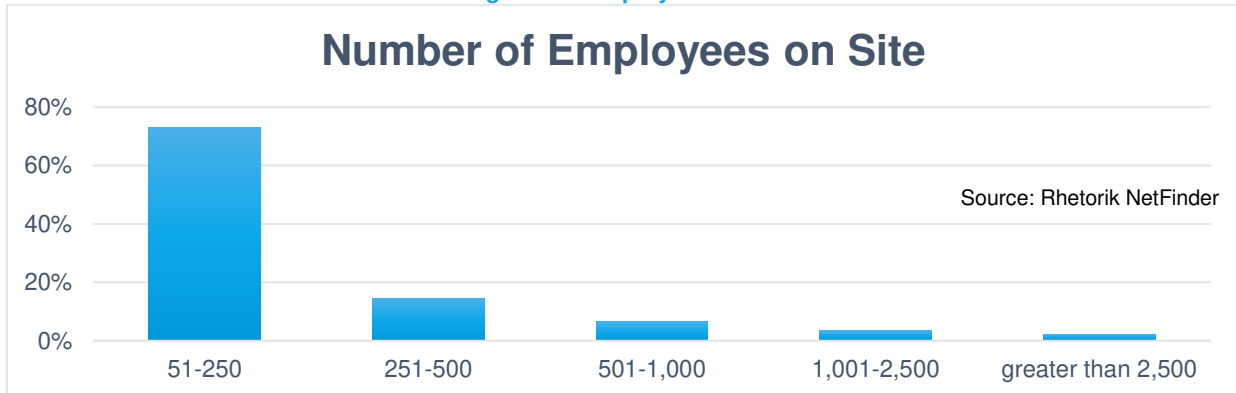
Services and Education have the largest market share with 31% and 12% respectively. These are followed by a broad distribution of different market sectors such as Wholesale, Construction & Contractors, Transport and Retail.

Significant industries in the “Other” sector include Insurance, Telecommunications and Utilities.

2.3 Profile by Employee Numbers

The NetFinder end-user base is made up of companies of various sizes. Figure 3 shows a breakdown by number of employees on site.

Figure 3 – Employees on Site



The majority of the sites profiled (73%) have between 51 and 250 employees on site, while a further 15% have between 251 and 500 employees on site.

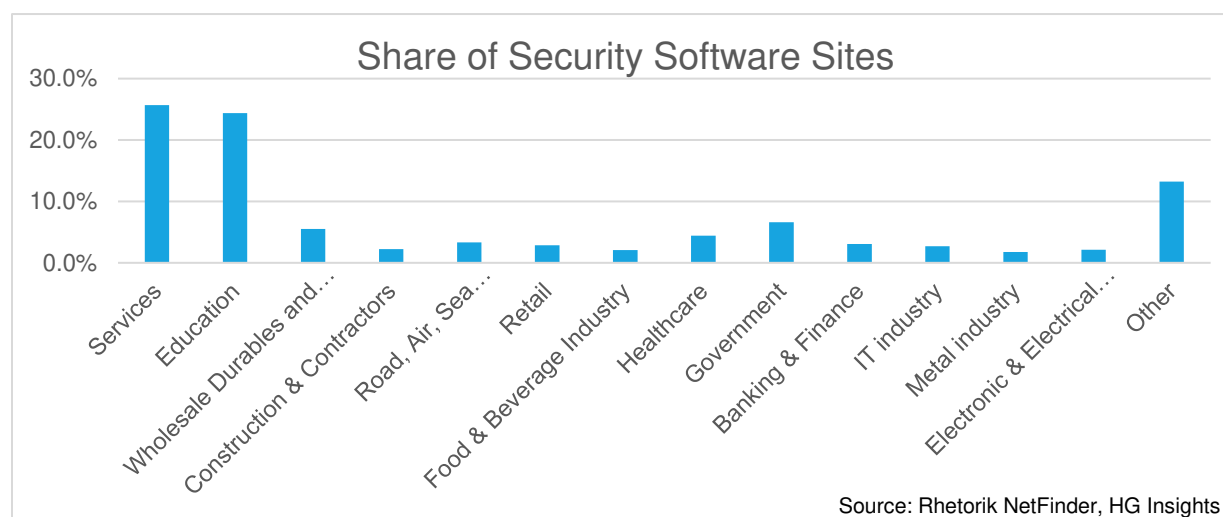
3. Profile of Security Software technologies

This section provides a summary profile of sites where the presence of at least one Security Software application has been identified.

3.1 Profile by Industry Sector

The Services and Education sectors contribute the most numbers of sites where a Security Software application has been detected. See Figure 4 for details.

Figure 4 – Share of Security Software Sites by Industry Sector



The industry sector shares of Security Software sites broadly reflect the overall make-up of the NetFinder database, but a closer look at the data reveals some interesting differences. Figure 5 shows which Industry Sectors are above or below the average penetration rate.

Here we see that the public sector (Education, Government, and Healthcare) and Banking & Finance are much more likely to have Security Software applications, especially compared to the likes of Construction & Contractors and Food & Beverage firms.

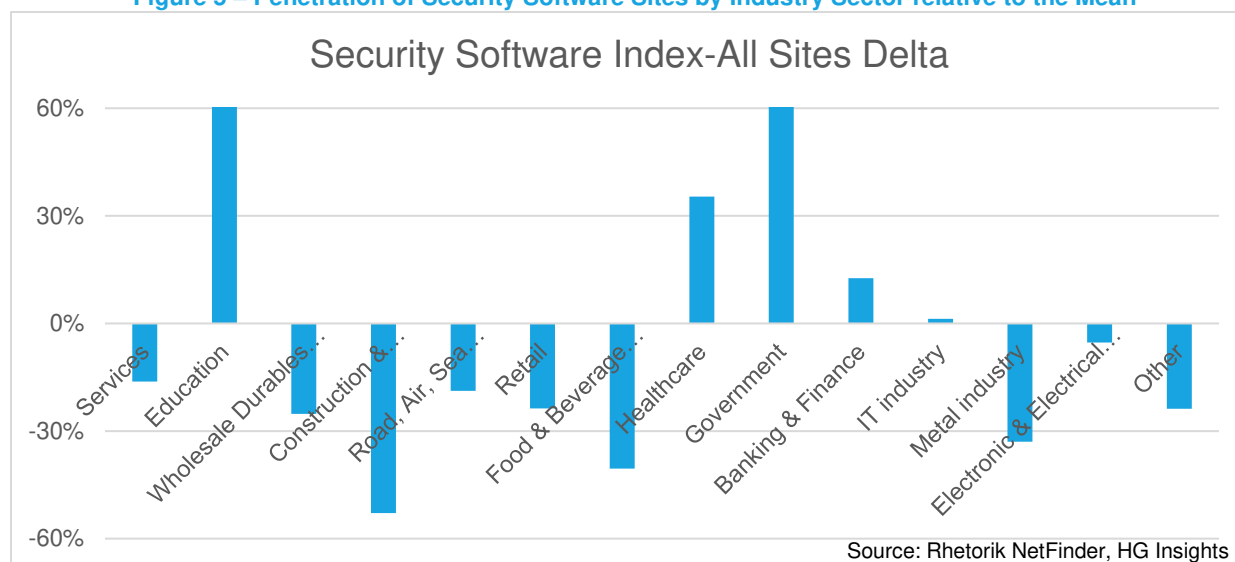
Interestingly, these high-presence sectors are rather similar to those identified in the National Cyber Security Centre (NCSC) 2019 annual review as being most “supported by NCSC Incident Management” – ie, those having been the targets of the most incidents: Government, Academia (Education), IT, Managed Service Providers, Transport and Health.



It is beyond the scope of this report to determine cause and effect, but it may be that the sectors with the highest penetration of security software applications have invested more heavily in these technologies because they are the most-targeted sectors.

Industry Sectors with large numbers of Sites but with low relative penetration, such as Services, Wholesale, Construction & Contractors and Transportation, offer Security Software vendors considerable opportunity for growth.

Figure 5 – Penetration of Security Software Sites by Industry Sector relative to the Mean



3.2 Profile by Number of Employees on Site

As with Industry Sector, the distribution of Security Software by number of employees on site broadly reflects the overall NetFinder database (see Figure 6).

Figure 6 – Share of Security Software Sites by Size

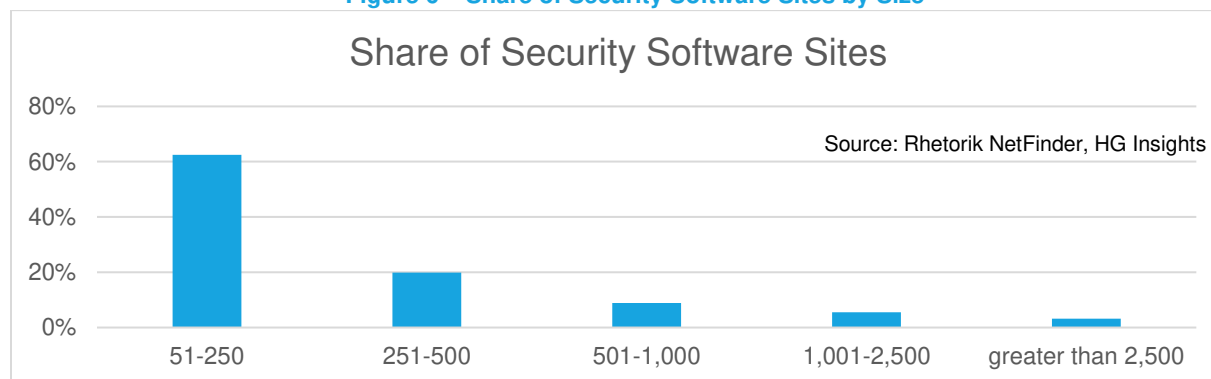
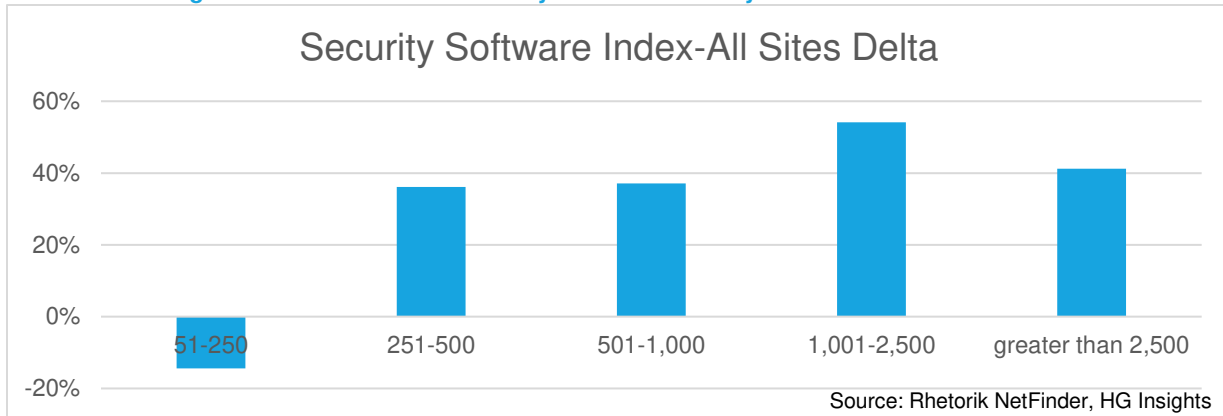


Figure 7 shows which Size bands are above or below the average penetration rate. Now we see that Sites with more than 250 employees are much more likely to have Security Software applications than Sites with less. This effect is most pronounced in the 1,001 to 2,500 employees on site band.

There is an opportunity for security software providers to grow their business within the 51-250 employee organisations.

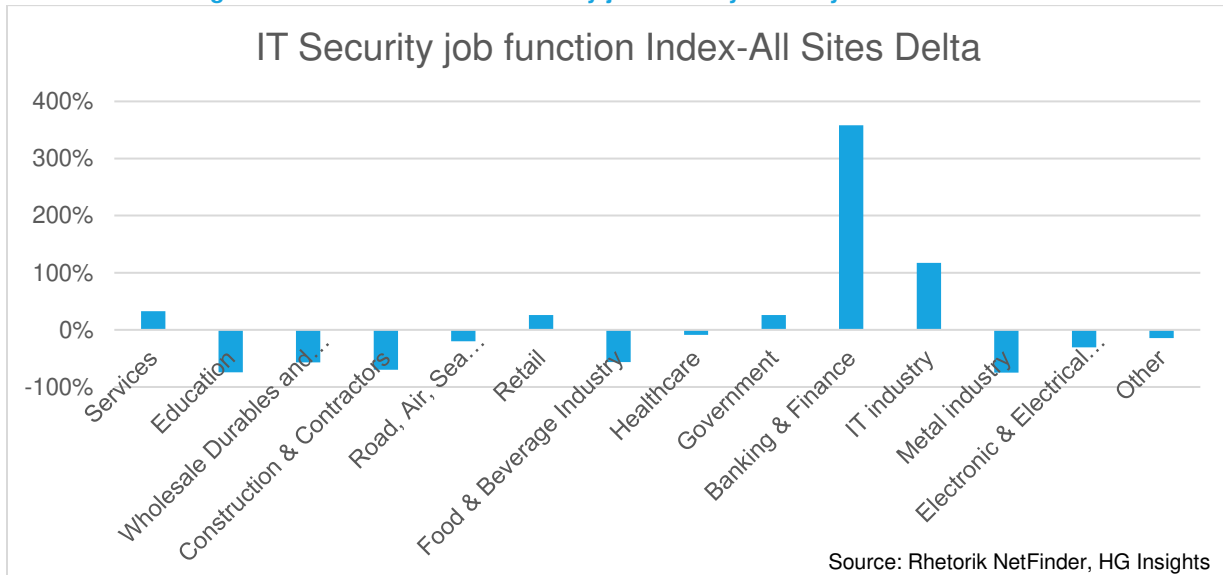
Figure 7 – Penetration of Security Software Sites by Site Size relative to the Mean



3.3 Profile by IT Security Job Function

An analysis of more than 180,000 contacts within the NetFinder database reveals which sectors are most likely to have a dedicated IT Security job function on site (see Figure 8).

Figure 8 – Penetration of IT Security job roles by Industry relative to the Mean

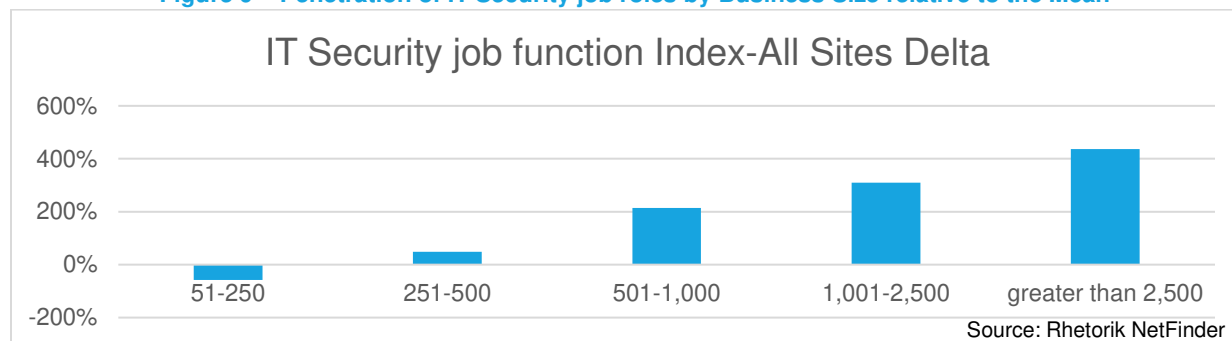


Services, Retail and Government all over-index relative to the average, and the IT Industry over-indexes significantly. However, the chart is dominated by the Banking & Finance sector, which is more than 3 times more likely than average to have a dedicated IT Security job function on-site.

A similar over-weighting can also be seen when looking at the prevalence of IT Security job functions by Business Size (Figure 9).

Here we see a strong correlation between prevalence and size, with the largest sites more than 4 times more likely than average to have a dedicated IT Security job function on-site.

Figure 9 – Penetration of IT Security job roles by Business Size relative to the Mean

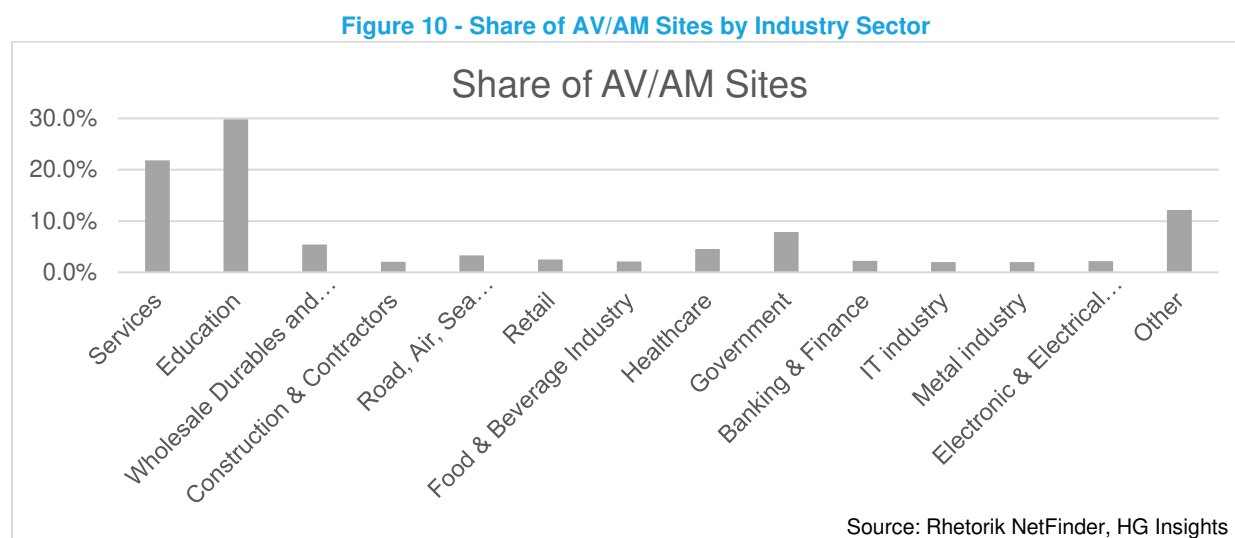


4. Antivirus and Antimalware Applications (AV/AM)

In this chapter we explore the presence of Antivirus (AV) and Antimalware (AM) Applications, one sub-category of Security Software, across the sample.

4.1 AV/AM Applications by Industry Sector

Figure 10 shows the share of sites in each industry sector where the presence of Antivirus and Antimalware Applications was identified.

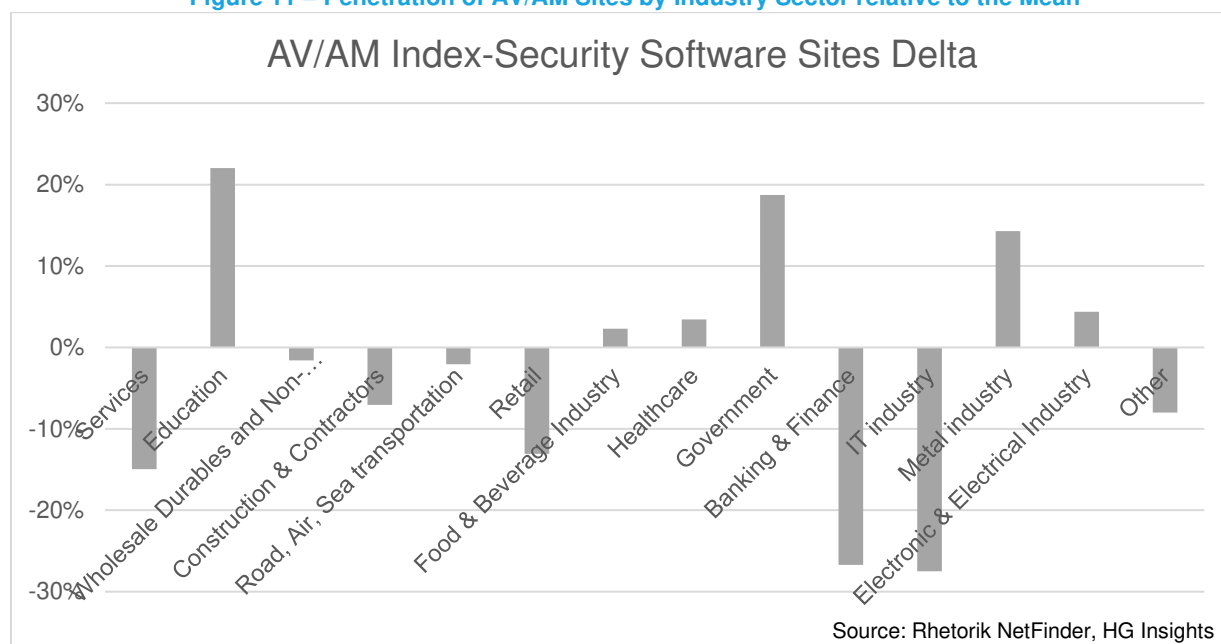


The Services and Education sectors contribute the most instances of AV/AM software identified, with Education and Government being more highly penetrated than other sectors.

This can be very clearly seen in Figure 11 below, where we look at which Industry Sectors have the highest likelihood of AV/AM presence.

A key difference to the overall Security Software picture is that the Services, Retail, Banking and IT Sectors are considerably below the average for AV/AM presence. Even the Healthcare sector does not over-index as much for AV/AM as it does for Security Software as a whole, suggesting there may be further opportunities here.

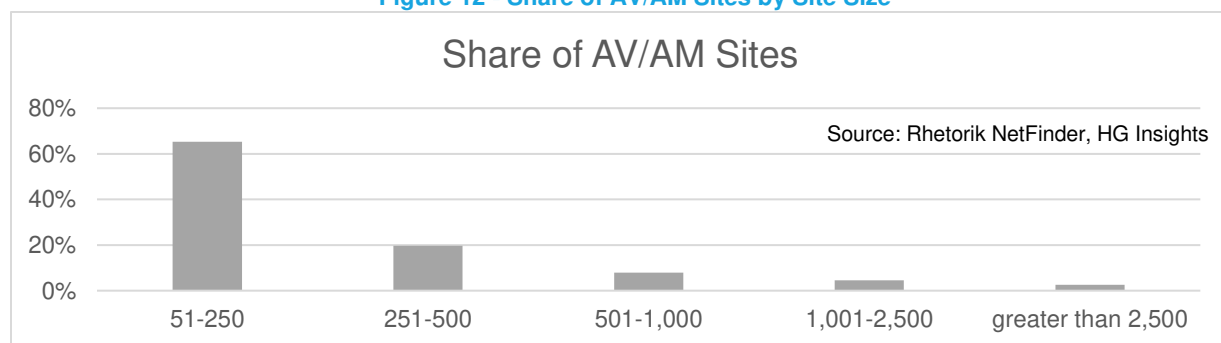
Figure 11 – Penetration of AV/AM Sites by Industry Sector relative to the Mean



4.2 AV/AM Applications by Number of Employees on Site

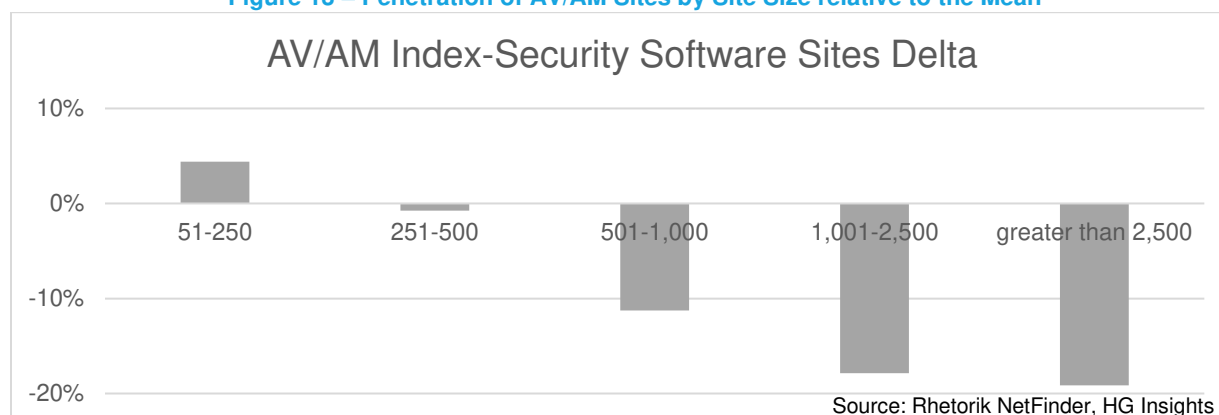
The share of Antivirus and Antimalware Applications presence by Site Size, as measured by the number of employees on site, is broadly representative of the NetFinder database.

Figure 12 - Share of AV/AM Sites by Site Size



When looking at the relative presence of AV/AM software by size, we see that it is negatively correlated. The larger the number of employees on site, the less likely there is for stand-alone AV/AM applications to be present (see Figure 13).

Figure 13 – Penetration of AV/AM Sites by Site Size relative to the Mean



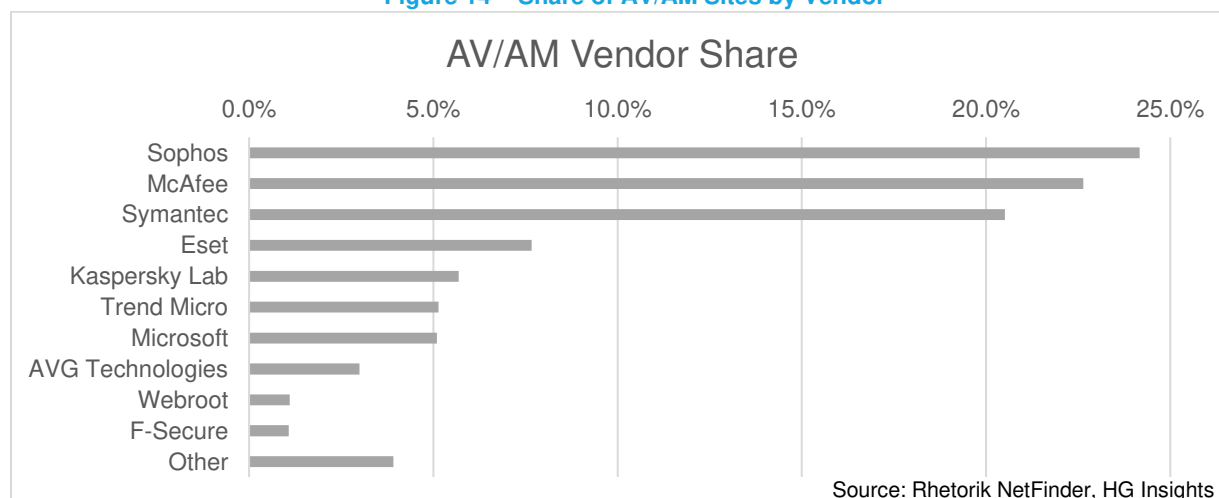
It may be that the larger sites tend to have more sophisticated cyber security technologies, which incorporate AV/AM functionality, rather than having stand-alone AV/AM technologies installed.

4.3 AV/AM Applications by Vendor

Sophos, McAfee and Symantec all have more than 20% share within the sample, with a gap back to Eset, Kaspersky, Trend Micro and Microsoft all in the 5-8% share range.

With 27 Vendors in total in the sample, and a Vendor Diversity Index of 54 out of 100, this market is moderately dominated by top vendors.

Figure 14 – Share of AV/AM Sites by Vendor

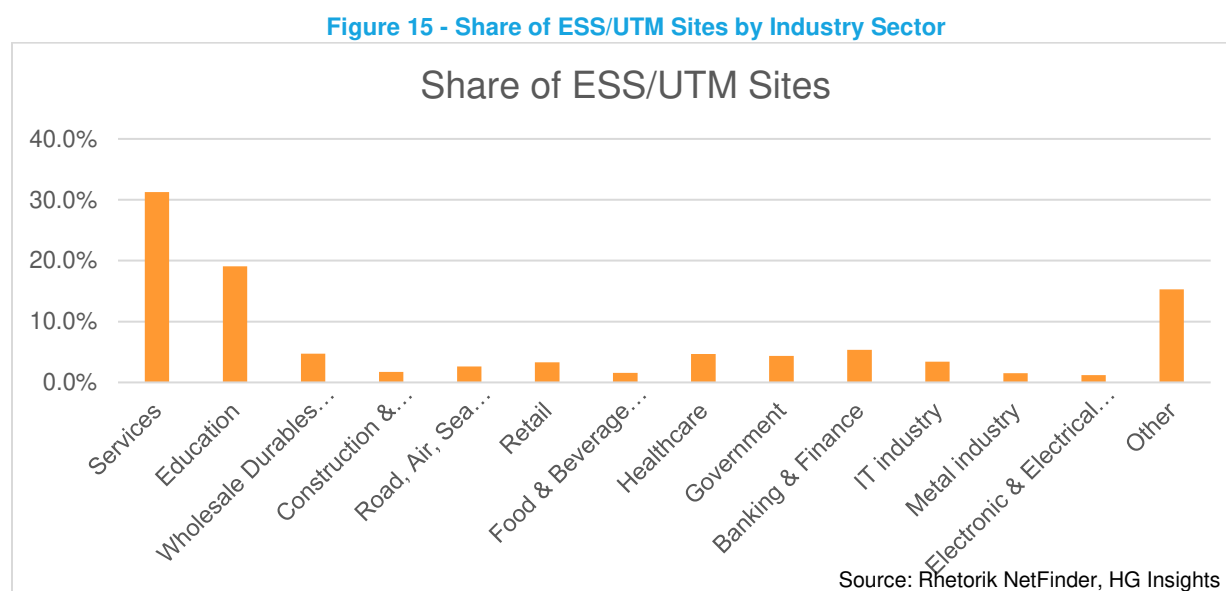


5. Endpoint Security Solutions and Unified Threat Management

In this chapter we explore the presence of Endpoint Security Solutions and Unified Threat Management (ESS/UTM) software, another sub-category of Security Software applications, across the sample.

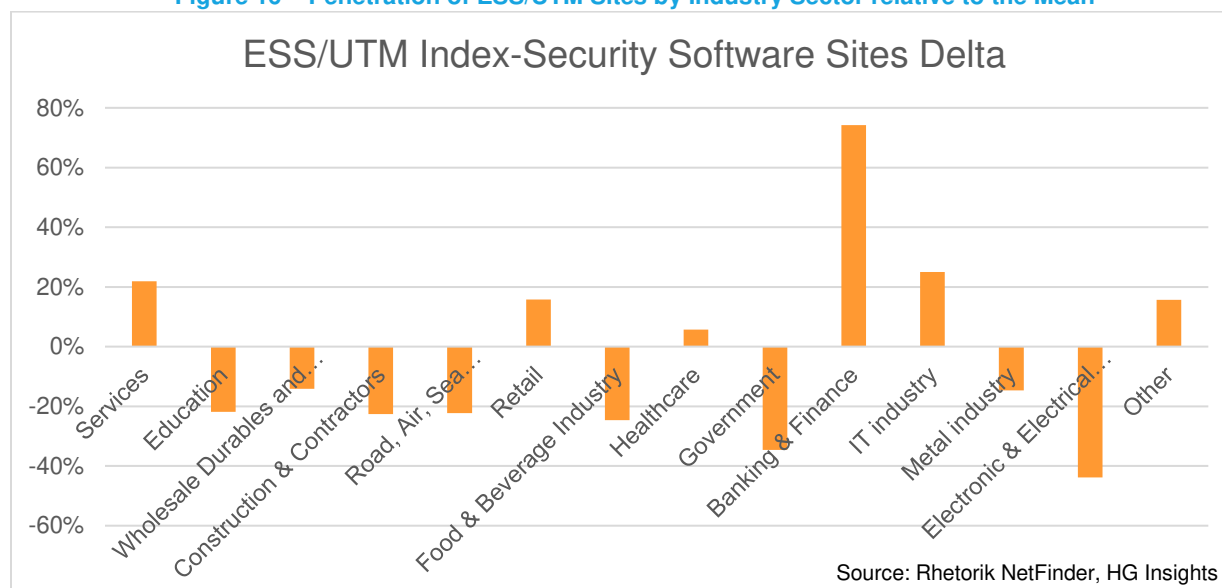
5.1 ESS/UTM Applications by Industry Sector

Figure 15 shows the share of sites in each industry sector where the presence of ESS/UTM has been identified.



When looking at the relative presence of ESS/UTM relative to the mean, we see a very different picture to Antivirus & Antimalware and to Security Software overall – Banking & Finance is highly penetrated, and Services and IT Industry also have above average penetration, while Government and Education are under-indexed, representing a healthy opportunity for ESS/UTM vendors.

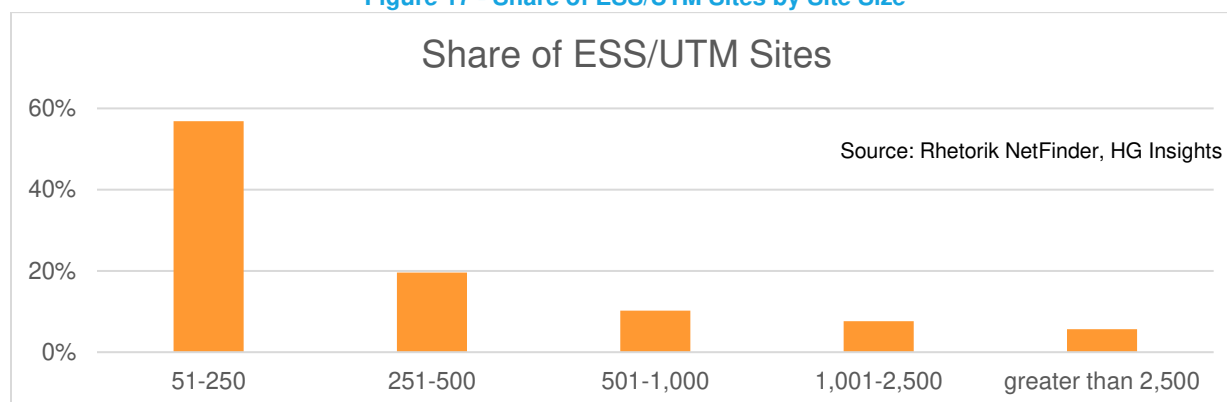
Figure 16 – Penetration of ESS/UTM Sites by Industry Sector relative to the Mean



5.2 ESS/UTM Applications by Number of Employees on Site

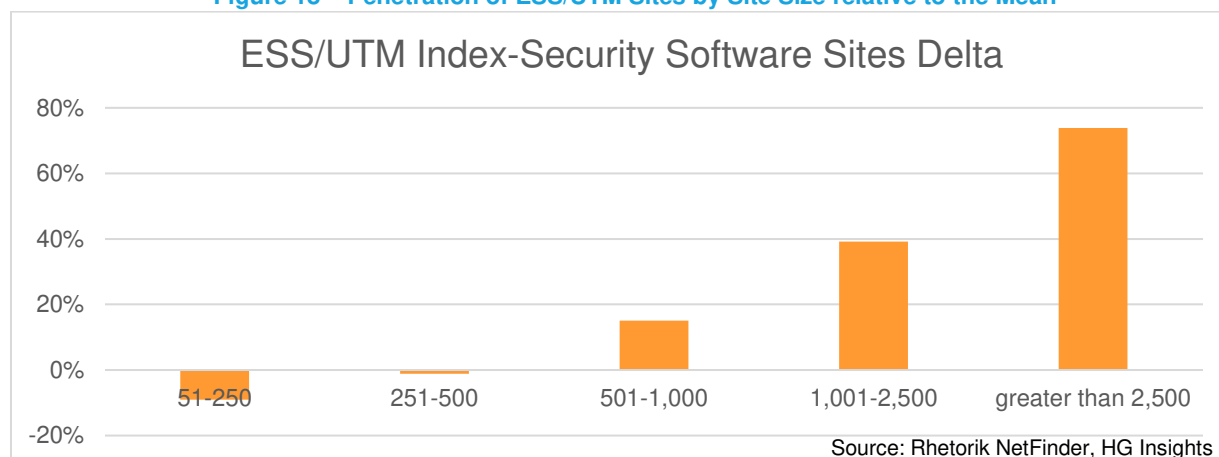
The share of Endpoint Security Solutions and Unified Threat Management presence by Site Size, as measured by the number of employees on site, is broadly representative of the NetFinder database.

Figure 17 - Share of ESS/UTM Sites by Site Size



When looking at the relative presence of ESS/UTM software by size, we see a very strong correlation – the larger the site, the more likely to have ESS/UTM detected (see Figure 18).

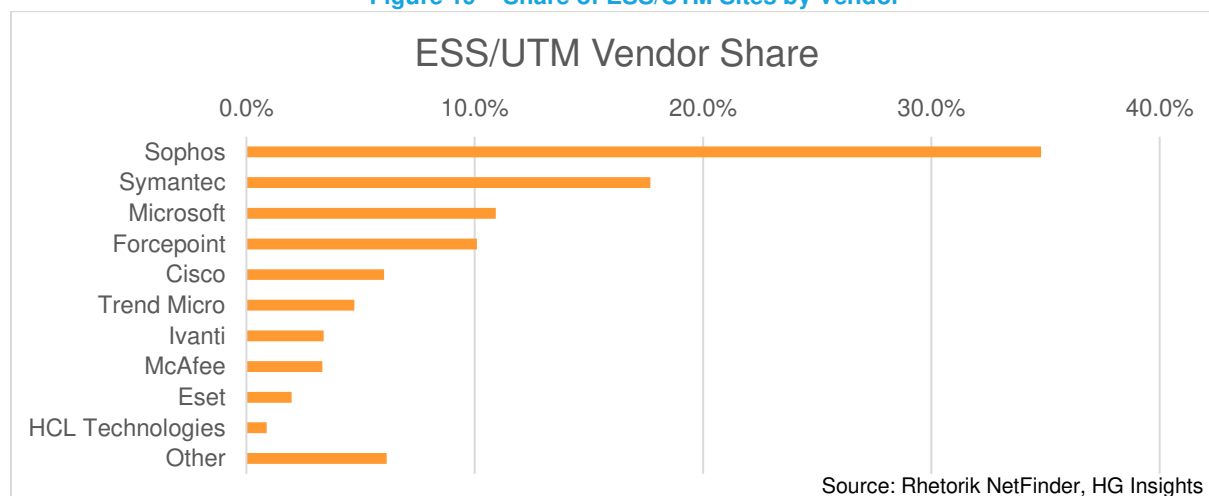
Figure 18 – Penetration of ESS/UTM Sites by Site Size relative to the Mean



5.3 ESS/UTM Applications by Vendor

Sophos is the most popular vendor within the sample, with almost double the share of Symantec, the next nearest vendor. With 30 ESS/UTM vendors in the sample, and a Vendor Diversity Index of 58, this is a market moderately dominated by top vendors.

Figure 19 – Share of ESS/UTM Sites by Vendor



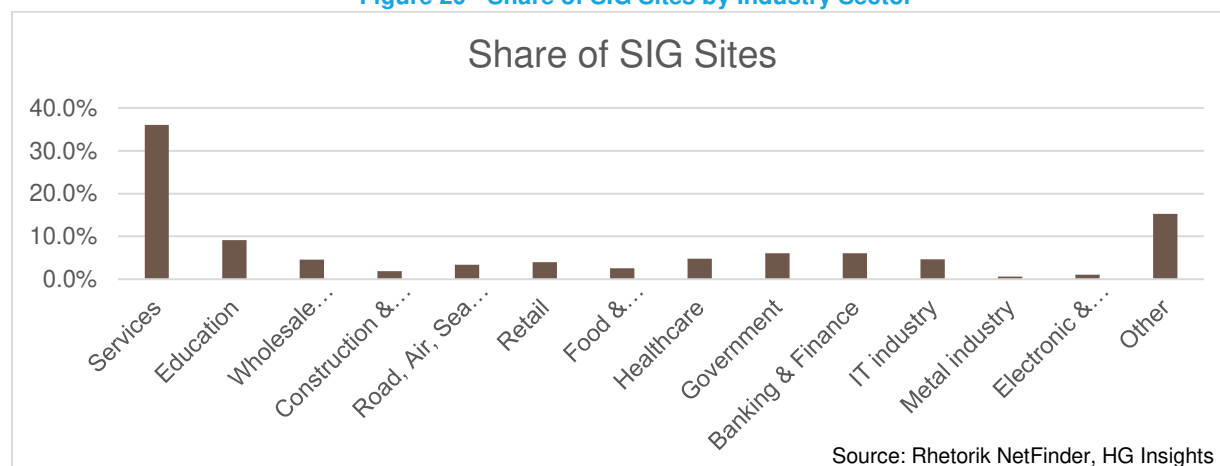
6. Security and Identity Governance

In this chapter we explore the presence of Security and Identity Governance (SIG) technologies, our final sub-category of Security Software applications studied for this report.

6.1 SIG by Industry Sector

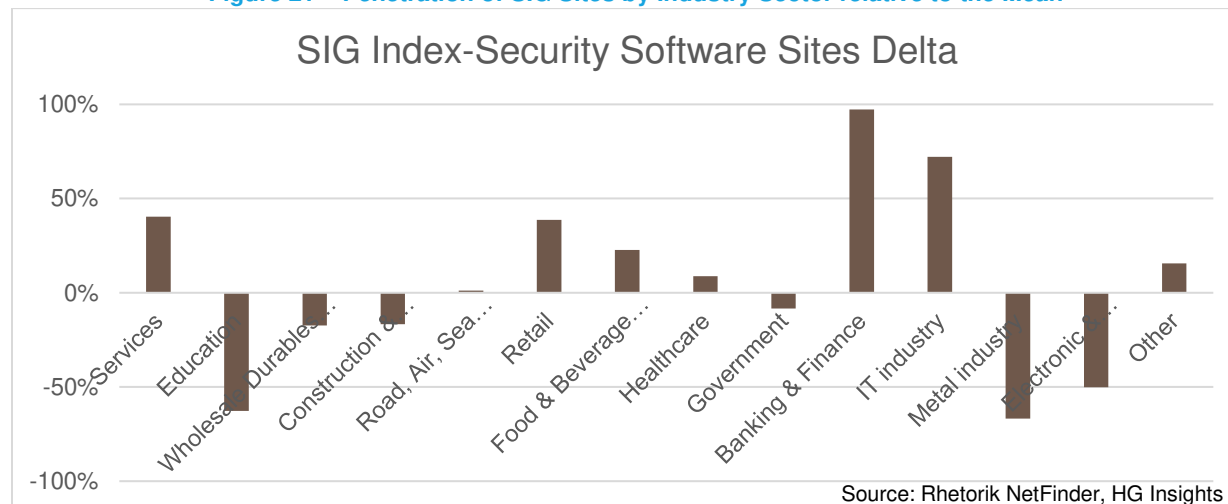
Figure 20 shows the share of sites in each industry sector where the presence of SIG software has been identified.

Figure 20 - Share of SIG Sites by Industry Sector



When looking at the relative presence of Security and Identity Governance software relative to the mean, we see rates are led by Banking & Finance, IT and Services, while Education is under-penetrated.

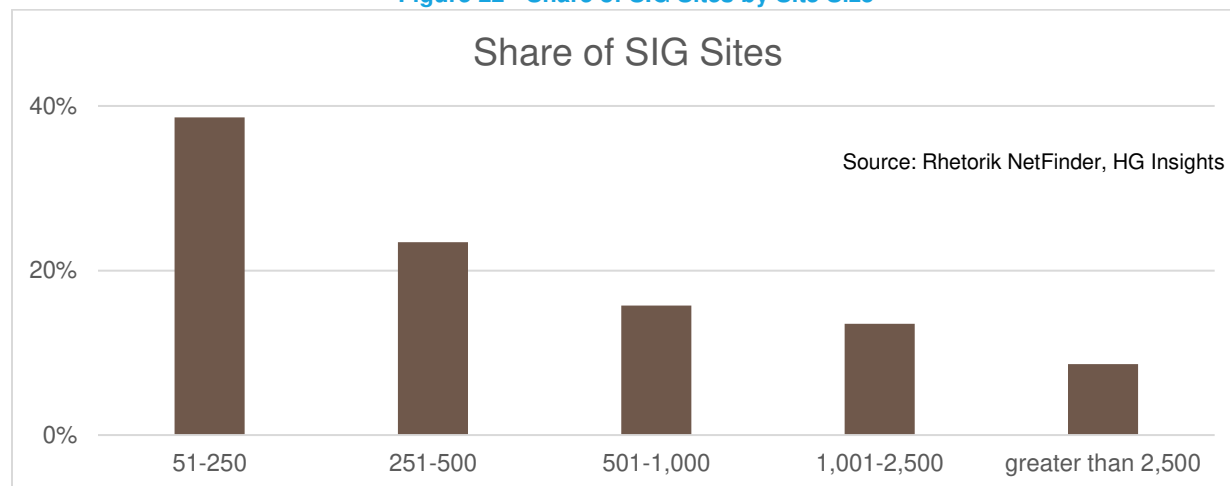
Figure 21 – Penetration of SIG Sites by Industry Sector relative to the Mean



6.2 SIG Applications by Number of Employees on Site

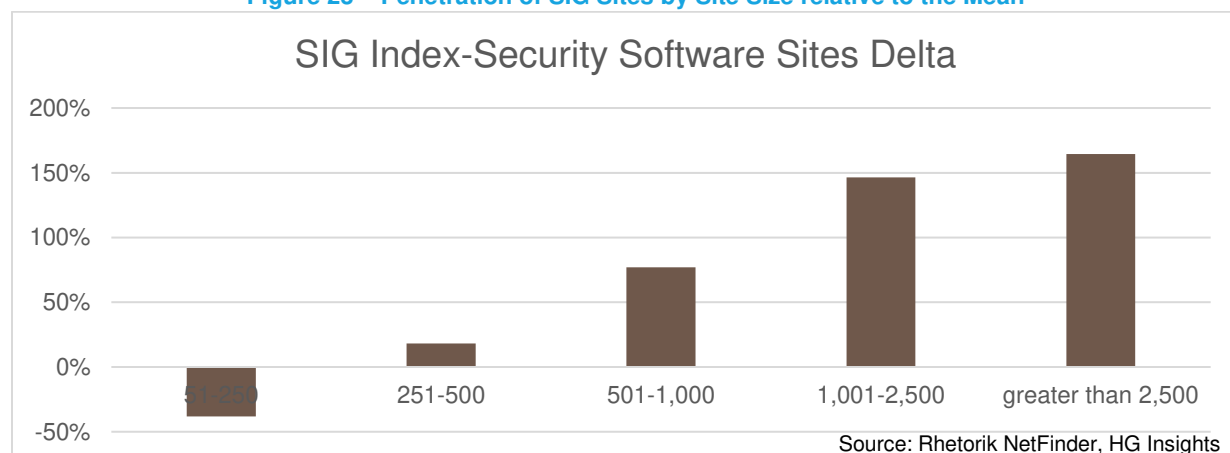
The share of Security and Identity Governance presence by Site Size, as measured by the number of employees on site, is broadly representative of the NetFinder database.

Figure 22 - Share of SIG Sites by Site Size



When looking at the relative presence of SIG technologies by size, we see a very strong correlation – the larger the site, the more likely to have SIG detected (see Figure 23).

Figure 23 – Penetration of SIG Sites by Site Size relative to the Mean

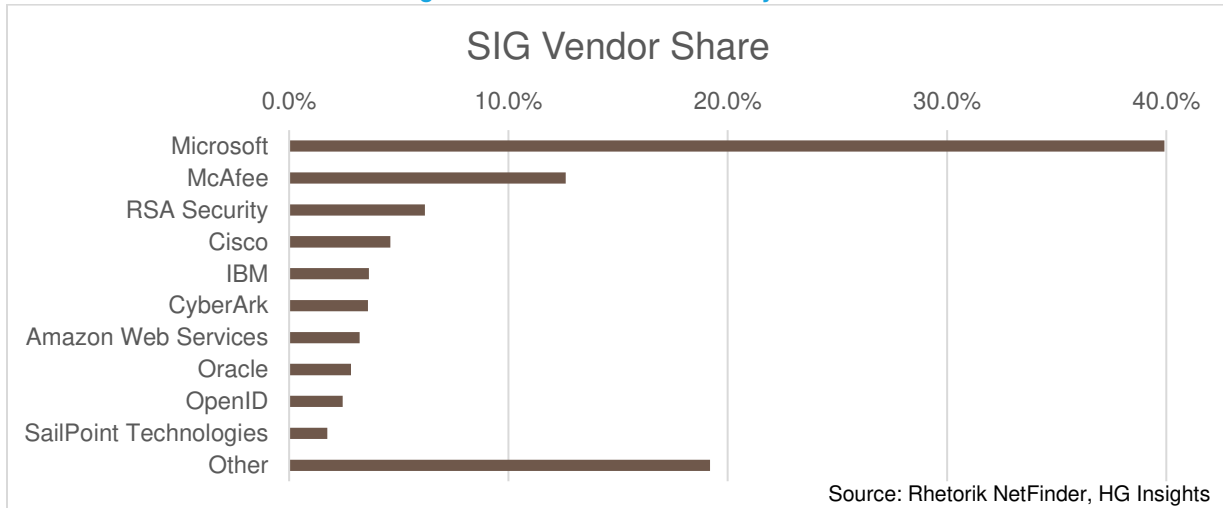


6.3 SIG Applications by Vendor

Microsoft dominates with 40%, with McAfee the next most popular in the sample at just under 13%. These are followed by RSA Security, Cisco, IBM and CyberArk

With 50 SIG Vendors in the sample, and a Vendor Diversity Index of 59, this is a market moderately dominated by top vendors.

Figure 24 – Share of SIG Sites by Vendor



7. Research Methodology

Rhetorik's dedicated team of NetFinder telephone researchers continuously monitor the products and services used by more than 50,000 end-user sites in the UK and Ireland. The research focuses on enterprise technology decision-making establishments with more than 50 employees on site. The inclusion of all vertical market sectors ensures coverage of all key enterprise technology investment.

The team collects and regularly updates information on the use of a broad range of products, services, brands and suppliers at each site, as well as maintaining information on the core details such as site name, address and key contact details. Together with licensed and mined data, this forms probably the most comprehensive and up-to-date continuous tracking survey of the enterprise technology end-user base in these countries today.

The information is gathered through primary telephone interview research, online surveys, data mining and data licensing. Technical details are gathered from key technology decision-makers at each site, typically IT and Telecoms managers and other senior staff directly responsible for purchasing and implementing the actual products and services in use.

In addition, technology data is provided by our data partner, HG Insights, the global leader in technology intelligence. HG Insights uses advanced data science methodologies to process billions of unstructured digital documents to produce the world's best technology installation information.

The research data is held in the comprehensive NetFinder database that can be licensed by clients to support their sales, marketing and business objectives. It can also be used for ad-hoc analysis of products, services and suppliers as well as for tracking the uptake of these same products, services, suppliers and brands over time.

8. About Rhetorik

Rhetorik is a global market intelligence company with 25+ years' experience offering data services to the IT, technology and telecommunications industry. We offer a range of data acquisition, enrichment and lead targeting services, specializing in international markets.

8.1 NetFinder™

Account and contact intelligence (technographics, firmographic profiling and enterprise technology decision-maker contacts):

- Geography – Data coverage across Europe, Asia Pacific and North America
- Technology – Unique technology marketing database: Tracking 12K+ technology products and solutions, from 6K+ vendors, across more than 150 categories.
- Methodology – Data gathered through multiple sources and methodologies to maximize breadth and quality: human called/curated, machine-crawled, surveyed, third party licensed from local sources, automated information handling and in-house phone verification

8.2 Rhetorik Data Services

Visit the Rhetorik DataClinik™ to maintain, enrich and enhance your data to cut costs, boost sales and marketing effectiveness and comply with data protection legislation

- Clean – clean your data by removing duplicate records, updating company and contact records (address, phone, email, title, etc), and validating existing data.
- Enrich – enrich your company and contact records with additional firmographics (address, URL, switchboard, employees, revenues, etc), technographics (technology assets across 12K+ products from 6K+ vendors) and contacts (technology decision makers, influencers and users), providing contextual data to aid segmentation, prioritization and messaging
- Comply - Reduce your compliance risks by keeping your companies and contacts data updated and maintaining up to date telephone preference service registrations, opt-outs and suppressions.

8.3 ROCKET™ – ABM Role targeting

Rhetorik's proprietary ABM role targeting tool maps the Technology decision making process to People (decision makers, influencers and users of technology solutions) in any industry, organisation and size of company.

- Assess the readiness and receptiveness of a given company towards your technology.
- Surface previously unknown contacts.
- Personalise messaging & channel selection.

8.4 Rhetorik Compliance Services

GDPR/e-privacy consultation and support with opt-in campaigns as needed



Rhetorik Enterprise Technology Market Report

For more details about Rhetorik's NetFinder database or Business Intelligence & Research Solutions, please visit www.rhetorik.com