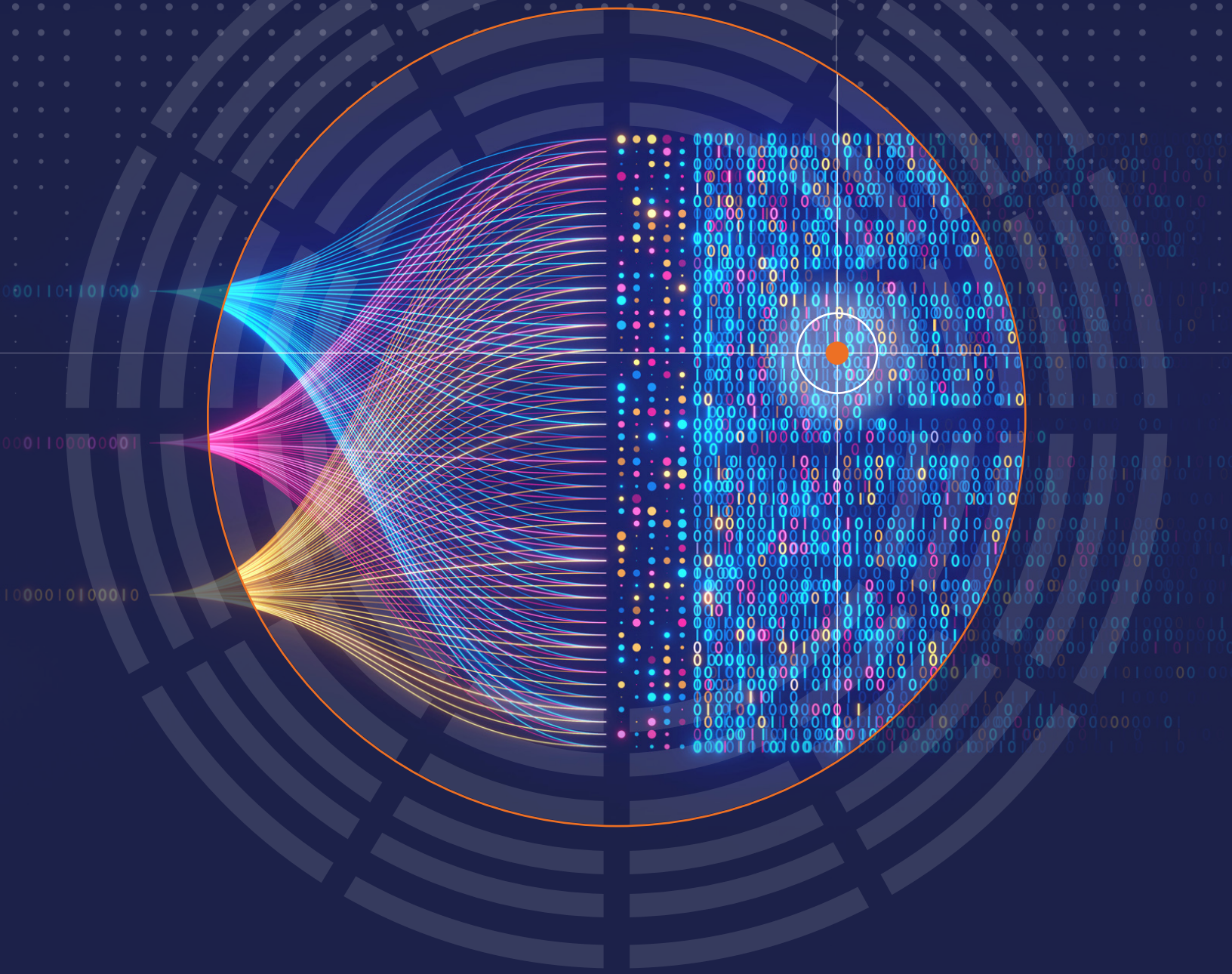
VIPRE SECURITY GROUP



Data Breach Kit

The ultimate guide on how SMBs can prevent a data breach

The ultimate guide on how SMBs can Prevent a Data Breach

Are SMBs all that different from large businesses? 03

Why do SMBs need to prevent data breaches? 04

How do data breaches happen? 05

- System intrusion 06
- Basic web application attacks 06
- Social engineering 07
- Miscellaneous errors 07
- Privilege misuse 07

What do cybersecurity agencies suggest? 08

- UK Cyber Essentials 08
- CISA Cyber Guidance for Small Businesses 08
- Australian Cyber Security Centre Essential Eight 08
- ENISA Cybersecurity for SMEs 08

How SMBs can prevent a data breach by addressing each breach pattern 09

VIPRE offers a flexible and layered approach 10

Layer 1: Email Security 11

Layer 2: Security Awareness Training 12

Layer 3: Endpoint Detection and Response (EDR) 13

How VIPRE can help 14

Are SMBs all that different from large businesses?

Small and Medium-sized Businesses (SMBs) account for 90% of companies, 60 to 70% of employment, and 50% of GDP globally[1].

They are the backbone of societies worldwide, contributing to local and national economies while sustaining livelihoods, especially among the working poor, women, youth, and marginalized groups.

More than ever, small businesses need support to overcome the ripple effects of geopolitical turbulence, climate crisis, and financial recession. Besides these threats, SMBs face increasing cyber risks as they rely on digital technology and services to innovate and gain an advantage in a competitive market. According to the World Economic Forum 2023 Global Risks Report[2], cybercrime and cyber insecurity are among the top 10 short- and long-term global risks.

SMBs require enhanced cybersecurity maturity because their attack surface has expanded during the last few years due to accelerated digitization. As a result, the latest Verizon 2023 Data Breach Investigations Report[3] highlights that SMBs and large enterprises increasingly use similar services and infrastructure. Cloud-based models and as-a-Service offerings have allowed small businesses to access technology that was previously beyond their reach. That has led to a convergence of attack surfaces regardless of the organization's size. However, due to constrained resources, the ability of small businesses to respond to threats and data breaches is very different.

Small businesses (less than 1,000 employees)	
Frequency	699 incidents, 381 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)

Table 3. At a glance for SMB

Large businesses (more than 1,000 employees)	
Frequency	496 incidents, 227 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat actors	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Internal (41%), Credentials (37%), Other (30%), System (22%) (breaches)

Table 4. At a glance for large organizations

Figure 1: Small and Large Businesses Comparison. Source: Verizon 2023 Data Breach Investigations Report.

[1] https://www.un.org/en/observances/micro-small-medium-businesses-day
[2] https://www.weforum.org/reports/global-risks-report-2023/
[3] https://www.verizon.com/business/resources/reports/dbir/

Why do SMBs need to prevent data breaches?

If we want to protect and strengthen our national economies, it is essential that we harden and secure the backbone; small and medium-sized businesses.

This is a crucial necessity because small businesses are the most vulnerable to the effects of a data breach – especially the financial ones.

According to Hiscox4 research from 2021, the average financial cost of cyber atacks to a US small business is $25,612; enough to significantly impact business continuity.

These costs include:

- Activities to reasonably detect a breach.
- Notifying affected individuals, data protection authorities, and other third parties.
- Post-breach communication and redress activities.
- Lost business opportunities and revenue due to system downtime.

Besides the tangible costs, small businesses must account for the hidden costs of a data breach, such as the time required to clean up the mess, the emotional, mental, and psychological impact on their employees[5], and the efforts required to rebuild trusted relationships with customers, partners, and suppliers.

Besides the above costs, data breaches may also involve compliance penalties for violating privacy requirements enshrined in respective regulations and acts. For instance, since GDPR enforcement began in May 2018, Data Protection Authorities (DPAs) have imposed fines with a cumulative total of €4 billion[6].

[5] These effects have been extensively covered in various academic publications. For example, see the research Psychological Data Breach Harms by Ido Kilovaty, University of North Carolina School of Law (https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1432&context=ncjolt) and the article Emotional Experiences of Cybersecurity Breach Victims at the PubMed Central (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8563455/)
[6] https://www.enforcementtracker.com/?insights

How do data breaches happen?

The latest iteration of the Verizon DBIR includes some interesting findings that every business, no matter their size, should study.

- The human element is involved in 74% of data breaches. The percentage includes mistakes, malicious insiders, misconfigurations, use of weak passwords, etc.
- 83% of the breaches are attributable to external actors, which means that insiders – employees, partners, and suppliers – are responsible for 17% of data breaches.
- Stolen credentials, phishing attacks, and vulnerability exploitation are the top three data breach vectors.
- Ransomware is not going away any time soon and is involved in 24% of data breaches.

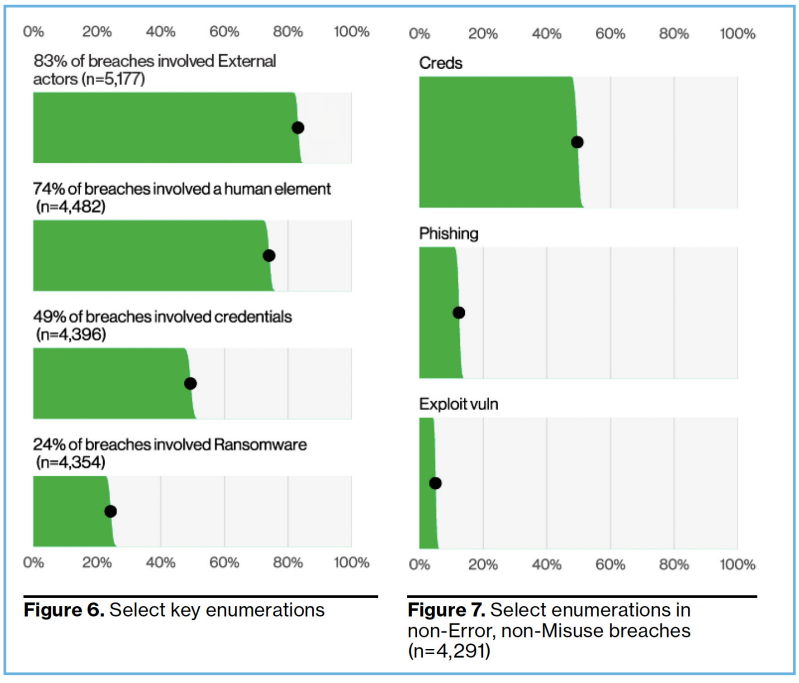


Figure 6. Select key enumerations

Figure 7. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

Figure 2: Verizon 2023 Data Breach Investigations Report Key Findings. Source: Verizon.

How do data breaches happen?

Examining the tactics and techniques criminals use to steal and compromise data is essential for small businesses to craft their defenses. Again, you can see the most common data breach patterns below:

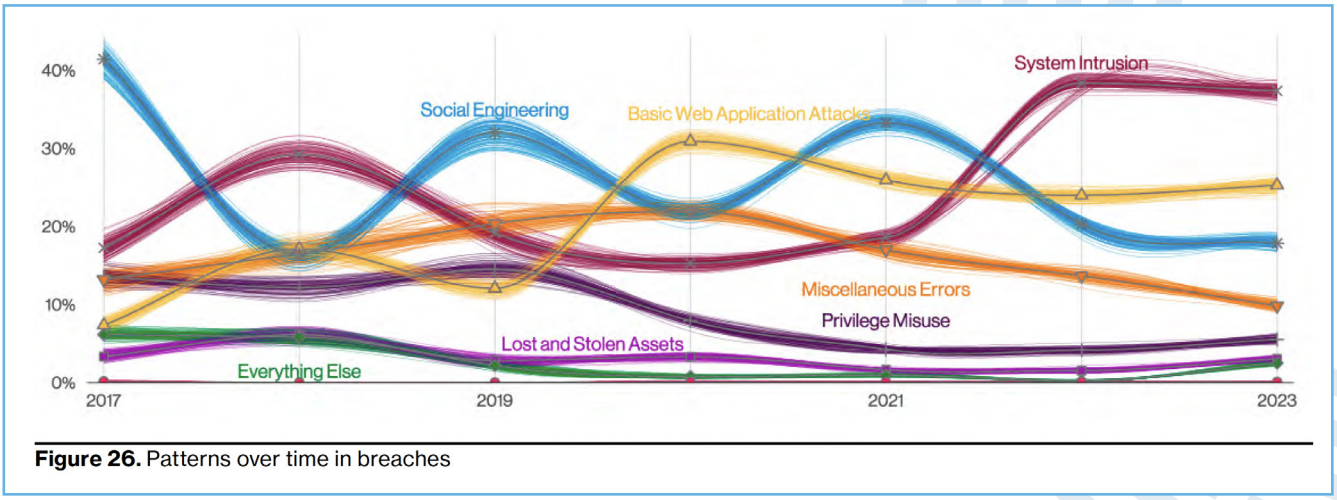


Figure 26. Patterns over time in breaches

Figure 3: Data Breach Patterns. Source: Verizon 2023 Data Breach Investigations Report.

System intrusion

System intrusion are complex attacks that leverage malware and/or malicious hacking to achieve their objectives. These attacks include deploying ransomware and exploiting unpatched vulnerabilities; hence, system intrusion has become the most common attack tactic. According to Verizon, “Malware is largely distributed via email and often comes in the form of Microsoft Office documents. Email as a vector isn’t going away any time soon. The convenience of sending your malware and having the user run it for you makes this technique timeless.”

Basic web application attacks

These attacks are against a public-facing web application; after the initial compromise, criminals do not perform many additional actions. It is the “get in, get the data, and get out” pattern. 89% of web app attacks involve the use of stolen credentials.

How do data breaches happen?

Social engineering

Social engineering involves the psychological compromise of employees to manipulate their behavior into breaching data confidentiality and integrity. Social engineers “use the information they have learned about you and your loved ones to trick you into believing the message is truly from someone you know, and they use this invented scenario to play on your emotions and create a sense of urgency.” Phishing and Business Email Compromise (BEC) attacks belong in this category with BEC accounting for 50% and phishing for 44% of all social engineering attacks.

Miscellaneous errors

These are incidents where unintentional employee actions compromise a security attribute of an information asset. Many unintentional insider incidents fall under this category, for example a data leak because of email misdelivery. It is vital to highlight that when employees with access to sensitive information commit errors, these mistakes can lead to costly and disruptive breaches. It is also likely that the vast majority of these types of incidents go unreported, as an employee “oops” moment will likely be swept under the rug until or unless there are obvious repercussions.

Privilege misuse

This is the case of malicious insiders. These incidents are driven by unapproved or malicious use of legitimate privileges. Malicious insiders are predominantly financially motivated.

What do cybersecurity agencies suggest?

To help SMBs avoid costly data breaches and safeguard their economies, various national and international cybersecurity agencies have developed and published comprehensive guides.

UK Cyber Essentials

UK National Cyber Security Centre (NCSC) has developed the government-backed Cyber Essentials[7] framework that aims to help protect organizations, regardless of their size, against a range of the most common cyber-attacks. The framework includes five technical requirements – firewalls, secure configuration, patch management, access control, and malware protection. Besides the apparent security benefits, being Cyber Essentials certified is a requirement for bidding for government contracts.

CISA Cyber Guidance for Small Businesses

US-based Cybersecurity and Infrastructure Security Agency (CISA) has published a guidance[8] that takes a different approach by breaking the tasks down by role, starting with the CEO. The guidance then details tasks for the Security Program Manager and the Information Technology (IT) team. CISA notes that while following this advice does not guarantee that SMBs will never have a security incident, it does lay the groundwork for building an effective security program.

Australian Cyber Security Centre Essential Eight

The Australian Cyber Security Centre (ACSC) has developed prioritized mitigation strategies, named Strategies to Mitigate Cyber Security Incidents, to help organizations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight[9], which have been designed to protect Microsoft Windows-based internet-connected networks. The Essential Eight include, as the name suggests, eight security practices spanning from application secure configuration and hardening to disabling macros, multi-factor authentication (MFA), patching systems, and backing up data.

ENISA Cybersecurity for SMEs

The European Union Agency for Cybersecurity (ENISA) conducted an analysis of the capacity of small and medium-sized businesses within the European Union to handle cybersecurity challenges[10]. The report includes recommendations and proposals for actions that EU Member States can take to help SMBs improve their cybersecurity posture. Additionally, a concise guide containing 12 practical high-level steps is provided for SMBs to enhance the security of their systems and business.

[7] https://www.ncsc.gov.uk/cyberessentials/overview
[8] https://www.cisa.gov/cyber-guidance-small-businesses
[9] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained
[10] https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes. The companion guide is available at https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

How SMBs can prevent a data breach by addressing each breach pattern

Although the SMBs attack surface resembles that of large enterprises, addressing the same cyber threats requires a different, more pragmatic approach.

Safeguards selected for SMBs should be implementable with limited cybersecurity expertise and designed to thwart general, non-targeted attacks. The principal concern of these enterprises is to keep the business operational, as they have little tolerance for downtime. The data they are trying to protect is not business-critical and principally consists of employee and financial information.

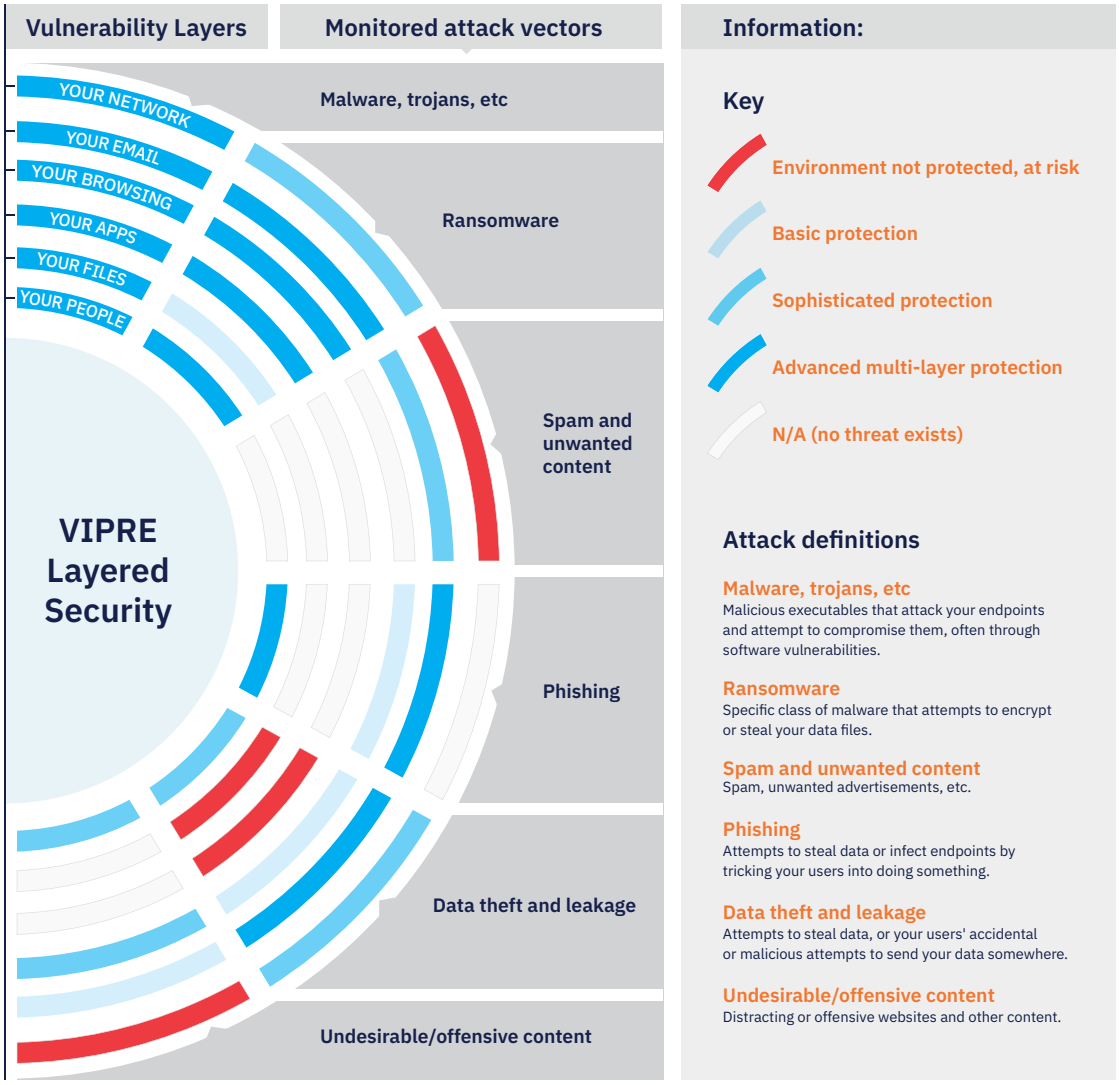
The biggest challenge in achieving this goal is the constrained environment of these companies – limited budgets, lack of experienced security professionals, and reliance on commercial off-the-shelf (COTS) hardware and software.

Cybersecurity guidance for SMBs would be most valuable if it addresses the patterns that criminals follow to reach and compromise data. By placing obstacles on the pathway to data, small businesses can prevent data breaches from happening.

VIPRE offers a flexible and layered approach

The next part of this guide follows a layered approach to cybersecurity and includes commercially available security tools and features to address the most common breach patterns analyzed above.

Layered cybersecurity is a pragmatic approach to protecting people, data, and systems and allows flexibility in addressing evolving cyber threats and managing human risks. Instead of following a monolithic and hard to sustain cybersecurity posture, a flexible and layered approach allows SMBs to become agile enough to be resilient against evolving and more advanced cyber threats.



VIPRE offers a flexible and layered approach

Layer 1: Email Security

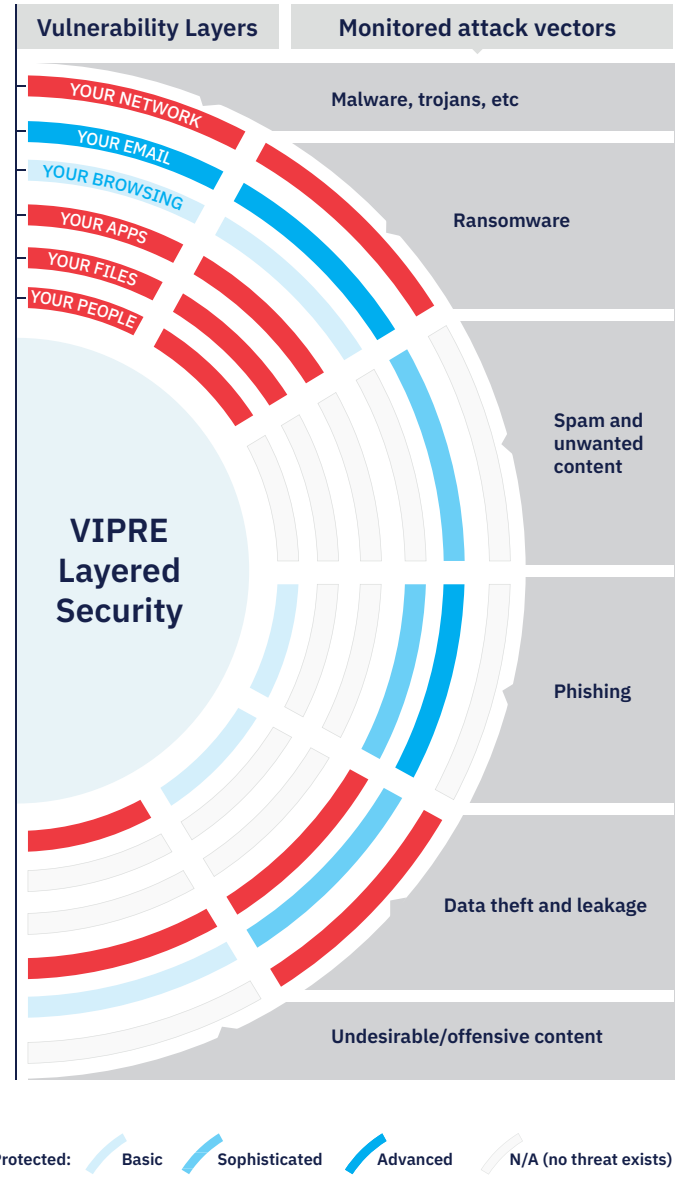
Email is the most targeted attack vector, and criminals leverage it to deliver phishing, BEC, and malware/ransomware attacks. A comprehensive email security solution should go beyond the basic protection offered by email vendors, such as Microsoft Outlook, to address sophisticated threats and attacks while preventing accidental disclosure of sensitive data through email misdelivery. If you are looking for an email security solution, make sure it offers the following capabilities to thwart phishing and BEC:

Email Security:

- Classic anti-spam, anti-phishing, and malware scanning to reduce the potential of bulk non-targeted attacks.
- Advanced Link/URL protection in the form of link isolation (rewriting) plus click-time deep content analysis using safe cloud sandboxing
- Advanced attachment sandboxing to analyze incoming messages for infected attachments in an isolated environment without risking the operational environment.
- Email encryption to ensure the integrity of your email communications with clients.
- Outbound recipient checks to check that only legitimate information leaves the company and reaches intended recipients.

With a comprehensive email security solution, SMBs can effectively protect:

- Their inboxes from malware and ransomware intrusion,
- Their people from phishing and BEC schemes, and
- Their data from accidental disclosure through misdelivery.



VIPRE offers a flexible and layered approach

Layer 2: Security Awareness Training

Cybersecurity goes beyond technology and processes to be effective. Cybersecurity is increasingly about managing human risks and empowering your people to recognize and react to threats that could potentially slip past email protections. The best way to address the human element of cybersecurity is by raising security awareness through a training program.

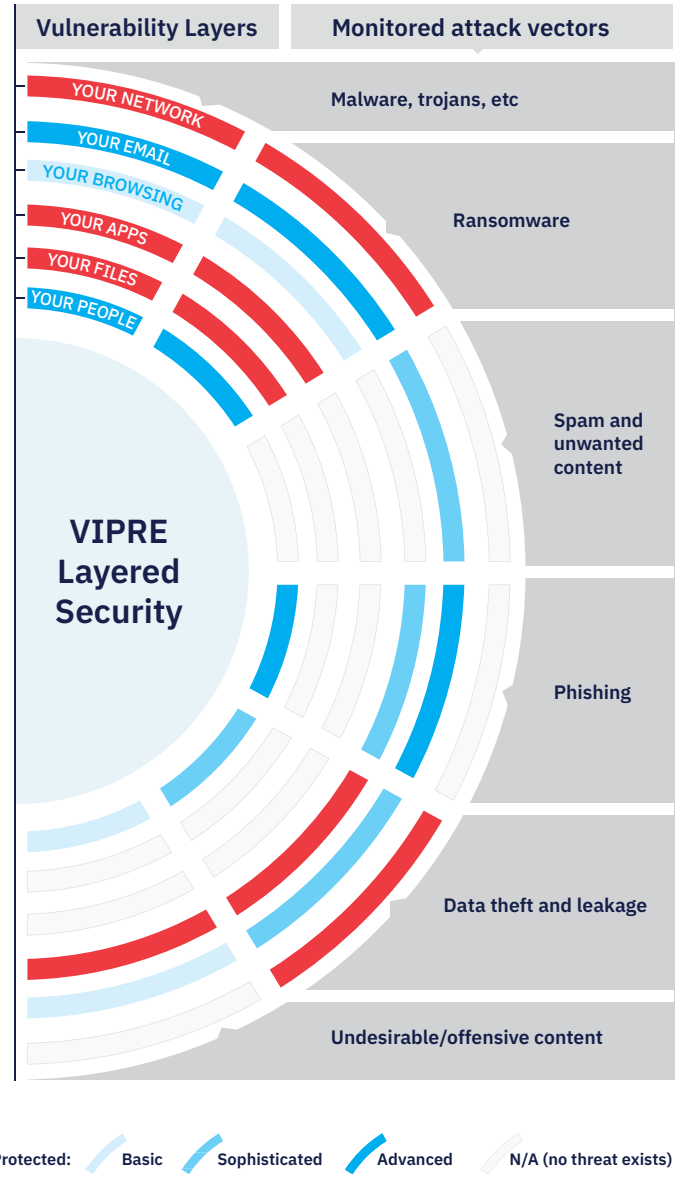
Although many vendors offer security awareness training, you should be looking for solutions that offer adaptive, customizable, and localized content, delivered in an engaging format to enhance motivation and knowledge retention.

When assessing a security awareness training vendor, look for the following features:

- The awareness content should cover security basics to empower people in cybersecurity and reduce the potential of accidental mistakes.
- Anti-phishing tactics and phishing simulations to address the phishing threat.
- Adaptive and gamified content to increase employee engagement.
- Engaging and localized content to motivate employees in reporting any abnormal or suspicious reporting and to create the context for a positive security culture.

A combination of email security and security awareness training greatly enhances the protection offered to an SMB. Besides protecting incoming and outgoing traffic, businesses manage the human risk more effectively and protect their people from sophisticated attacks.

Layer 1 and Layer 2 will help protect against many attacks and safeguard the business, however it is vital that SMBs add an additional protective layer to protect their ecosystem – network, files, and apps.



VIPRE offers a flexible and layered approach

Layer 3: Endpoint Detection and Response (EDR)

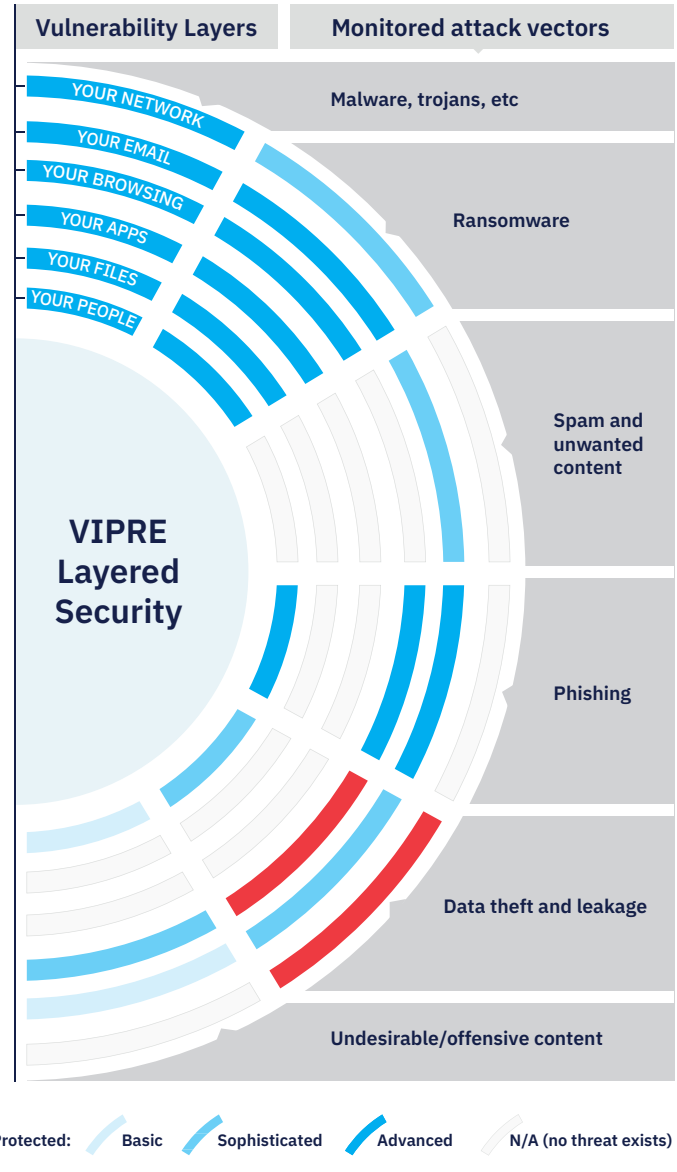
Should an attacker manage to sneak past the protections of email security and the human firewall, businesses need a third security layer to detect and block the threat if it makes it to your endpoints. This is the job of Endpoint Detection and Response (EDR). An EDR solution not only helps detect threats that slipped through the cracks, but also investigate and remediate the attacks on all the endpoints – applications, smart devices, cloud instances – a small business has. In addition, an EDR solution should be simple but robust enough to uncover suspicious behaviors and provide reporting integrated within the normal business workflows.

Many SMB's turn to Managed Detection and Response (MDR); a service that provides security monitoring and management. MDR helps rapidly identify and limit the impact of threats without the need for additional staffing.

These are the features you should be looking for:

- Robust antivirus process, file, and registry scanning to detect sophisticated malware on the endpoint.
- Machine learning-driven behavior monitoring to spot abnormal and suspicious actions on your endpoints and in your network.
- Network detection, analysis, and protection to discover lateral movements across your environment.
- Detailed attack telemetry to support investigation of potentially ongoing attacks.
- Containment and remediation tools either embedded or integrated, to support killing suspicious sessions and processes, removing malicious content, and direct remote endpoint access.
- Patch and vulnerability management to harden your endpoints and close any security gaps, future-proofing your endpoints.

The combination of all three layers provides the most comprehensive security for SMBs, reducing the potential and impact of a successful data breach.



How VIPRE can help

VIPRE offers a comprehensive portfolio of security solutions tailored to the small and medium-sized businesses to help prevent data breaches. On top of robust security, you will enjoy superb support and avoid the risks of vendor sprawl.

- **VIPRE Endpoint Detection & Response (EDR)** delivers a high-performing yet lightweight, cloud-based solution with built-in advanced machine learning for superior threat detection.

- **VIPRE Email Security Advanced Threat Protection** offers next level email security protection with attachment sandboxing and link isolation to combat spam, spoofing and security breaches with the convenience of cloud-based email security management.

- **VIPRE SafeSend** allows employees to confirm external recipients and attachments in Microsoft Outlook, and also scans outgoing emails and attachments to ensure sensitive data does not leave your network.

- **Inspired eLearning Security Awareness Training** powered by VIPRE delivers engaging security-focused, customizable, and localized educational content to enhance motivation and knowledge retention and empower your employees in cybersecurity.

Figure 4: VIPRE Product mapping

To discover what VIPRE can do for your business, get a free demo or speak to an expert.

VIPRE SECURITY GROUP

North America
sales@vipre.com
+1 855 885 5566

UK and other regions
uksales@vipre.com
+44 (0)800 093 2580

DACH Sales
dach.sales@vipre.com
+49 30 2295 7786

Nordics Sales
nordic.sales@vipre.com
+ 45 7025 2223