SILENT BREACH

White Paper

Building an Effective Cyber Security Strategy

Contents

Introduction *3*

Our Approach: In Four Parts *5*

Phase 1: Monitor **5**

Benefits of Attack Surface Management 6

Phase 2: Defend **7**

Vulnerability Audits and Penetration Testing 7

Cloud Security 8

Social Engineering 9

Dark Web Assessments 10

Phase 3: Respond **10**

Business Continuity Planning 11

Post Incident Activity 12

Phase 4: Compliance **13**

Impact Assessments 14

Introduction

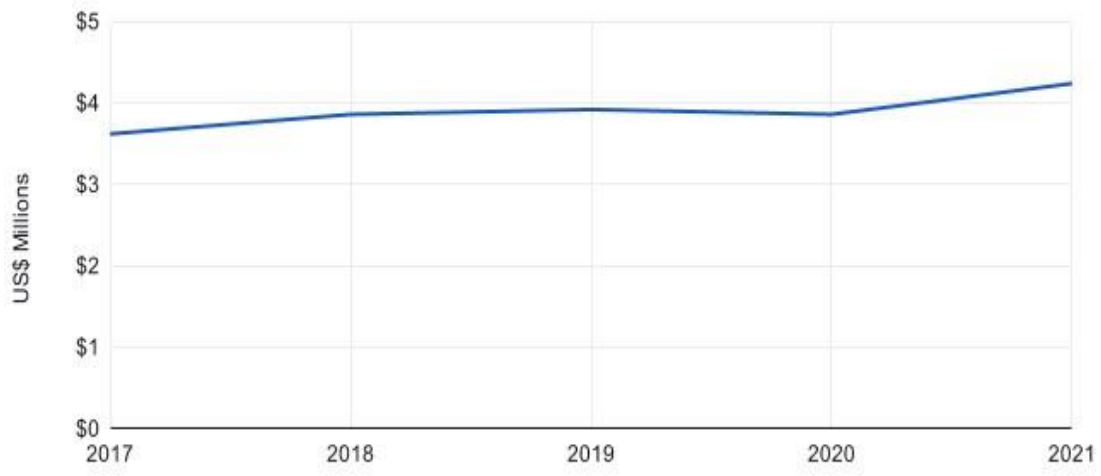
The average global cost of a data breach in 2021 was over $4 million, while the international cost of cybercrime has hit $6 trillion annually.

A major contributor to this upward trend is the delayed response times plaguing most industries. According to IBM, victims that respond to data breaches in under 200 days spend an average of $1.1 million less on data breach damages.

This is concerning because the average number of days required to identify and contain a data breach is 287, placing the vast majority of organizations in the upper pricing range.

This major pricing factor has been poorly addressed in cybersecurity programs across industries causing data breach costs to rise each year.

Average Cost of a Data Breach 2015 – 2021



Data source: Cost of a Data Breach Report 2021 (IBM and Ponemon Institute)

While most companies understand the new risks that have been introduced, many still struggle to articulate a solid cyber security strategy to fend off attacks and keep their businesses safe.

This White Paper breaks down the process of building an effective and innovative cybersecurity program that is capable of providing robust protections against most major existing threats while remaining flexible enough to adapt to emerging risks and opportunities.

In collaboration with our experts, clients, and partners, we've isolated the following six key requirements for an effective cybersecurity strategy. Our approach is:

- Realistic

  As your business evolves, your cyber security needs will evolve too. A realistic cyber security plan is flexible and can grow as your business grows.
- Incremental

  Learn to walk before you run. As your business grows, your cyber security capabilities must grow along it, adapting to new threats, new challenges, and new opportunities.
- Scalable

  Want to move to offensive security? Need to protect against DDoS? Want to meet ISO 27001 compliance? Build a strategy that can be easily and quickly upgraded.
- Foundational

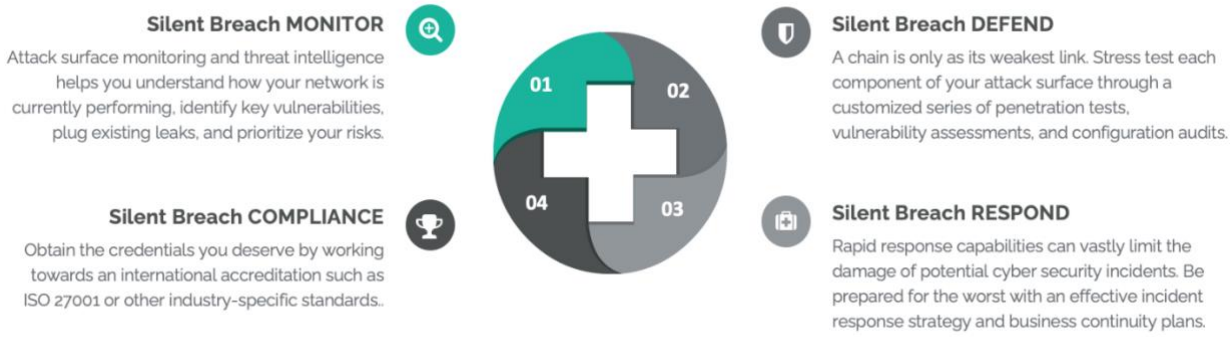
  Have no existing cyber security plan? No problem. Our approach helps companies build their cyber security strategy from the ground up and go from zero security to a security hero.
- Complimentary

  Already have a mature security plan in place? Continuously improve and work towards international compliance, demonstrating to your stakeholders and customers that you take security seriously.
- Guided

  Being a CISO is tough, and you need all the help you can get. Silent Breach can assist you every step of the way, helping you achieve and exceed your cyber security goals.

Our Approach: In Four Parts

Our step-by-step program is divided into the following four steps:



Phase 1: Monitor

Attack Surface Management is a central piece of cyber security planning and strategy. Your attack surface is the sum of every attack vector that can be used to breach your perimeter defenses. In other words, it is the total quantity of information you are exposing to the outside world.

Typically, the larger the attack surface, the more opportunities hackers will have to find a weak link which they can then exploit to breach your network. Unfortunately, your organization's attack surface can be quite large, thereby exposing you and your customers to a wide array of security threats.

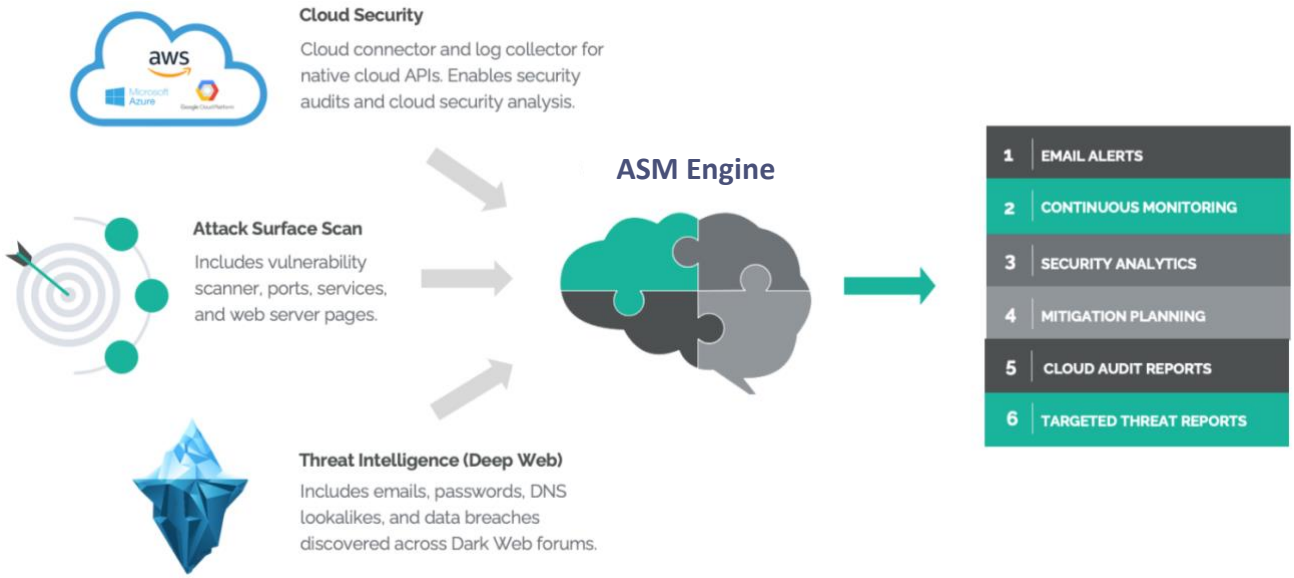
The key to effective attack surface management is to reduce your attack surface as much as possible, without compromising other business functions in the process.

Benefits of Attack Surface Management

Attack Surface Management solutions like Quantum Armor you allow you to:

- **Establish baseline security**: Generate a comprehensive map of your digital ecosystem.
- **Identify vulnerabilities**: Discover, track, and mitigate key vulnerabilities across your network, as well as data leaks and emerging threats
- **Security road-mapping**: Prioritize risks and generate remediation plans
- **Track security efforts**: Monitor the patching effort in real time to measure the efforts deployed by the infosec team
- **Regular audits**: Rate your attack surface once mitigation efforts have been applied

A typical ASM solution will comply with the following logical structure:



Phase 2: Defend

A chain is only as strong as its weakest link. Stress-test each component of your attack surface through a customized series of penetration tests, vulnerability assessments, and configuration audits.

You can prepare for an incident while safeguarding access to sensitive parts of your application through a number of steps, including:

- Deploying a WAF
- Configuring access control policies
- Security orchestration

Once deployed, your security measures will inspect and filter all incoming web traffic. In the event of an incident, they'll block any malicious request, issue an alert and document details about the attempt in an aggregated security log.

Here, relevance and granularity are key. Having access to a detailed security event description, you'll be able to understand incidents and provide the most appropriate responses.

Depending on the WAF, evidence can be collected and presented in real-time, enabling a nearly instantaneous, data-driven response to any attack attempt.

Vulnerability Audits and Penetration Testing

Penetration testing is a simulated attack on your network, orchestrated by a certified security engineer or group of security engineers to attempt to compromise your network and digital assets. The goal is to expose existing flaws and discover how your infrastructure and security team would cope with a real-life attack. At Silent Breach, our Penetration Tests are divided into three stages:

- **Security Testing**
  - Perform all remote and on-site tests, including social engineering and any additional security services.
- **Report & Remediation**
  - Provide detailed reports at the end of each test with technical tips to remediate any identified issues.
- **Re-test**
  - Re-test to confirm remediation is correctly implemented or risk has been accepted. With Silent Breach, re-tests are always included free of charge.

Cloud Security

The cybersecurity landscape has become incredibly complex, and cloud security has continued to evolve to keep up with emerging threats. Whether you're migrating to a cloud infrastructure platform for the first time or would like to harden your existing network architecture, it’s critical to maintain and enhance your organization's cloud security.

This must be done across **six key segments**:

- **Network Security**
  - **Includes:** Firewalls, IDS/IPS, web layer security, Bastion Hosts, Private & Public, Subnets, External Connectivity.

- **Data Security**
  - **Includes:** Encryption Mechanisms, Data, Resilience, Data Replication, Data Availability, Data Integrity

- **User Access**
  - **Includes:** API Access, User Access, Federated, Access Authentication Mechanisms, Authorization Mechanisms

- **Event Management**
    - **Includes:** Security Assessments, Proactive threat monitoring. Logging & Analysis, Notifications, Traffic pattern analysis.

- **Disaster Recovery**
    - **Includes:** Replication Mechanisms, Failover techniques, Minimizing service interruptions, Impact Assessments.

- **Business Continuity**
    - **Includes:** Business Impact Analysis Threat Modeling, Risk Assessments, Security Awareness, Tabletop Exercises.

Social Engineering

While social engineering has been around for decades, in recent years we've noticed a concerning uptick in the quantity and quality of social attacks. Cybercriminals use social engineering in 98% of attacks. There are 75 times as many phishing websites as malware sites. Incredibly, 75% of companies worldwide were victims of phishing in 2020.

It's more important than ever to perform regular social engineering simulations. At Silent Breach, for example, our award-winning experts are trained in both social psychology as well as tactical cybersecurity to ensure that you'll be prepared against the very best social hackers.

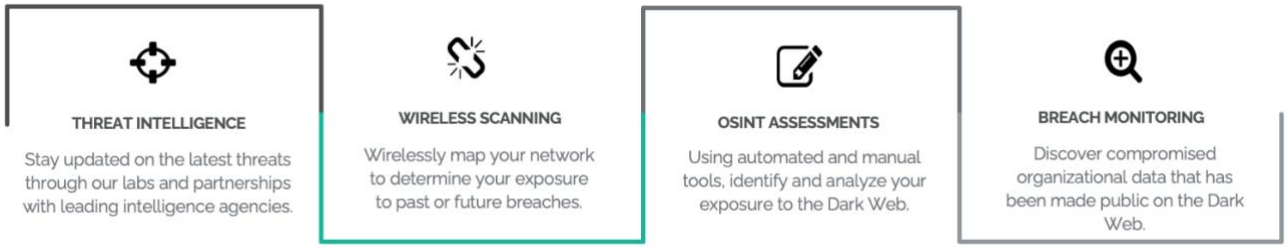
Using simple, yet effective techniques, Silent Breach ethical hackers have found that a layered attack — combining phishing, vishing, as well as targeted spearphishing attacks — can critically breach 90% of businesses within one week, all without writing a single line of code.

However, we've found that with the proper training and preparedness, companies can quickly reduce successful social engineering attacks by up to 80%.

Dark Web Assessments

The Dark Web is an unindexed and anonymous part of the Internet which is not accessible via standard browsers or search engines. The anonymity of the Dark Web gives cybercriminals cover to plan and launch cyberattacks on your infrastructure and data. Silent Breach uses cutting-edge intelligence to help you detect and respond to threats originating on the Dark Web.

Dark Web Services Snapshot

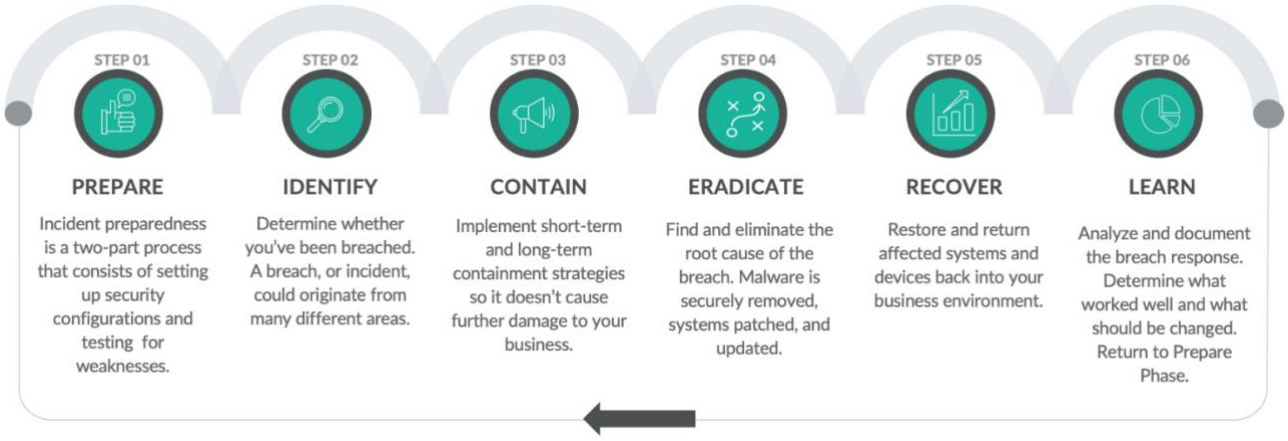


Phase 3: Respond

Nearly half of all SMBs have experienced a cyber incident in the last year alone. Of these, only 14% had the proper capabilities to detect, defend, and respond to the attack. On average, it takes up to 6 months for SMBs to detect a breach, leaving hackers with ample time to escalate their access, exfiltrate any valuable data, and escape undetected. Unfortunately, current trends indicate that it is not a question of *if* your company will be attacked, but *when*.

Incident Response services help organizations secure their networks by constantly monitoring network systems for malicious activity.

Our analysts implement the following IR Life Cycle to enable your organization to detect and respond quickly and effectively to a wide range of cyber threats.



Business Continuity Planning

The actions taken in the first few hours following a breach will continue to have large ramifications throughout the remainder of the recovery, for better or for worse. It is therefore critical to have an up-to-date and comprehensive Business Continuity Plan in place early on.

Business Continuity Planning (BCP) is a multi-stage process which creates a system of prevention and recovery from potential threats. The plan ensures that personnel and assets are protected and can function quickly in the event of a disaster. Our consultants are ISO 22301 certified and are ready to help you define your business continuity needs and strategy.

While the average data breach costs close to $4 million, Ponemon's latest Cost of a Data Breach Study estimates that having a Business Continuity Plan will save you $365,000 on average. On a per-file basis, the savings comes down to about $15 per compromised file.

Accordingly, business continuity planning is not only recommended, but can also shield your organization from liability in the event of a compromising incident.

Although BCPs should be specially tailored (in consultation with your cybersecurity partner) to your organization's needs and abilities, most IT BCPs should include the following 3 sections:

Post Incident Activity

Learning from the incident response is a four-part process:

1. Encourage feedback from responders at every level. First, second, and third line SOC operators and incident handlers each have a unique perspective that must be incorporated into future response playbooks.
2. Review all relevant documentation to ensure compliance. This includes organizational policies or regulatory mandates to ensure any disparities are addressed.
3. Chronicle any unanticipated or unusual events to extend procedures to mitigate similar occurrences in the future.
4. Annotate enhancements to existing processes that were identified during the incident response cycle.

Phase 4: Compliance

Obtain the credentials you deserve by working towards an international accreditation such as ISO 27001, NIST-CSF, HIPAA, PCI-DSS or other industry-specific standards.

Privacy and security regulations are often complex and it can be difficult to maintain compliance. They establish the users' right to know whether any of their data is being collected, sold, or disclosed. Furthermore, companies must demonstrate their ability to secure customer data from accidental or malicious leaks. Finally, companies will often need to provide the user with the ability to access or delete their data, or simply say no to its sale.

Awareness and Communication

Develop an Information Security Policy so that all employees understand the relevant standards and understand the proper communication channels to ensure proper data handling.

In addition, Silent Breach can help develop a culture of privacy within the company to implement data protection by design and by default.

Audit & Analysis of Personal Data

Silent Breach can help you analyze and track sensitive data through storage and processing, as well as determine data ownership roles.

Protect Private Data

We can help develop an IT strategy to implement data protections, backups and a rescue plan to guarantee business continuity in case of a data breach.

Access Rights & Customer Consent

Guidance in obtaining proper and legally valid consent from your customers. Our legal partners help guarantee that data is gathered correctly and is fully compliant with privacy guidelines.

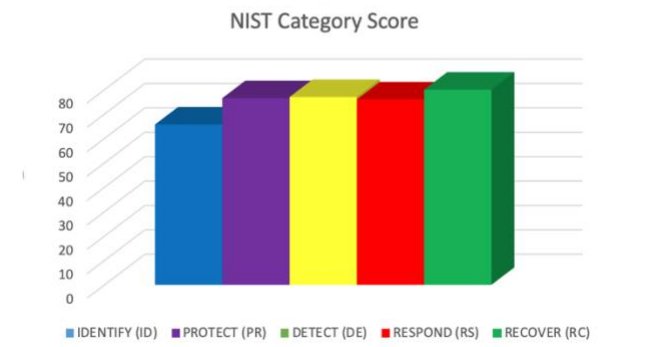
Appoint a Data Protection Officer

Many firms experience difficulty with creating this newly mandated role. Silent Breach can help select the best internal resources to act as DPO as well as assist in building a support team.

Impact Assessments

Understanding threats and evaluating the likelihood of an attack is extremely valuable. Creating a threat model allows you to clearly establish the angles any attacker would be likely to use and evaluate the risk for each attack vector. Threat modeling is an essential step towards risk mitigation, and repeatable risk assessment procedures.

NIST Threat Modeling provides a snapshot across 5 core areas.



The results are then translated into individual risk values.

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Questions? We have answers.

We're here to help, shoot us an email at:

hello@silentbreach.com

Looking for a better, smarter way to protect your data and prevent breaches?

Silent Breach offers a full suite of products for security, risk and vendor management teams.

Trusted by hundreds of companies worldwide

www.silentbreach.com

+1 727-497-7941

100 S. Ashley Drive, Tampa, Florida 33602