ONVETRIX LLC

Bringing Cybersecurity to the Cloud for Modern Businesses

Businesses are moving their operations into the cloud and threat actors taking notice. Secure your success with this eBook.

Businesses need to make cybersecurity a priority before it's too late.

Cyberattacks have been steadily increasing and show no signs of slowing down. Since the first recorded ransomware attack in 1989, delivered via floppy disk, cyber threats have only grown more frequent and sophisticated. Despite this, many business owners still believe they are too small to be targeted by cybercriminals. This misconception can be costly.

For businesses outside the tech sector, cybersecurity might not always be a top priority. With so many competing demands, it often falls lower on the list of concerns, but it shouldn’t. According to Verizon, 43% of all data breaches target small to medium-sized businesses (SMBs), yet only 14% of those businesses are prepared to defend against an attack. The consequences of a breach are often catastrophic. In fact, 60% of SMBs that suffer a cyberattack close their doors within six months due to the devastating impact on both their reputation and operations.

In today's digital world, every business, regardless of size, is a potential target, and preparing for cyber threats should be a critical part of every company's strategy.

43%
of attacks are aimed at SMBs *(Verizon)*

254%
increase in ransomware attacks in 2023 *(Microsoft)*

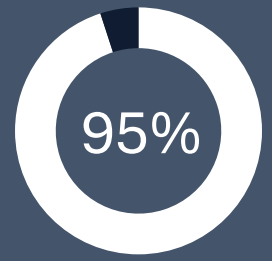
277
Days on average to identify and contain a breach *(IBM)*

300%
increase in the cost of cybercrime over the past 10 years *(Cybersecurity Ventures)*

The Real Cost of Cyber Crime for SMBs

Financial Loss

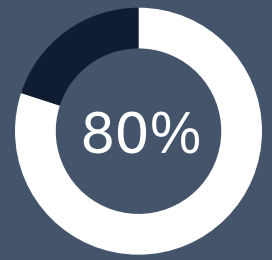
- A cyberattack can result in **immediate financial loss**, as cybercriminals often steal money through tactics such as ransomware, phishing schemes, and fraudulent transactions. These direct thefts can be devastating, especially for small and medium-sized businesses.
- The cost of **recovering from a breach**, however, often exceeds the initial financial loss. Businesses must bear the expenses of restoring systems, legal fees, regulatory fines, and compliance costs. These can quickly add up and, in many cases, become the largest financial burden. **According to SIBM's 2023 report, the average cost of a data breach globally is $4.45 million**, underscoring the immense financial impact that even a single breach can have on an organization.



Verizon's 2023 Data Breach Investigations Report, 95% of breaches that resulted in significant financial loss involved external actors.

Reputational Damages

- Failing to safeguard customer data can severely **undermine trust and loyalty**, causing lasting damage to a business's reputation. When customers feel their personal information is not secure, they are less likely to continue doing business with the company, which can result in lost sales and diminished credibility.
- High-profile cyberattacks often attract widespread media attention, intensifying the negative impact on a company's **public image**. This exposure can lead to a significant loss of market share, as competitors take advantage of the situation.



A study by *Cisco's 2023 Data Privacy Benchmark* found that nearly 80% of consumers would stop doing business with a company following a data breach.

The Real Cost of Cyber Crime for SMBs

Operational Disruptions

- Cyberattacks can rapidly cripple business operations, often bringing entire systems to a halt. The resulting downtime can last anywhere from days to weeks, or even months, depending on the severity of the attack. During this time, critical business activities are interrupted, causing delays in services, production, and customer support.
- Cyberattacks may lead to the loss or corruption of essential data, which can have long-term effects on how your business functions. Losing access to customer information, financial records, or operational data can disrupt workflows, hinder decision-making, and damage relationships with clients.

Legal and Regulatory

- Businesses can face severe fines after a data breach, such as **up to $7,500 per violation under the California Consumer Privacy Act (CCPA) or $60,226 per violation under HIPAA**.
- Breached businesses face class-action lawsuits, FTC investigations, and fines, with mandatory breach notifications required under state laws—failure to comply can result in additional legal penalties and reputational damage.

$5,600/minute

Gartner estimates that the average cost of IT downtime is $5,600 per minute, which can add up to $300,000 per hour for larger businesses, depending on the size and industry.

$1.2 million

According to *Deloitte's 2023 Global Data Breach Survey*, over 50% of organizations reported facing regulatory scrutiny or fines after a data breach, with the average legal and regulatory cost of a breach amounting to $1.2 million.

Most Common Threats Businesses Face

Cloud Security

Common vulnerabilities like misconfigurations, weak access controls, and insufficient monitoring make cloud environments prime targets for cybercrime. **Blackpoint Cyber reports seeing cloud attacks 10 to 1 over on premises cyber-attacks.**

Phishing Attacks

Phishing is a common and effective cyberattack where criminals use deceptive emails and websites to steal sensitive information or spread malware. **According to *Verizon's 2023 Data Breach Investigations Report*, 74% of breaches involved human error, such as falling for phishing scams**.

Ransomware

Ransomware attacks have surged, with businesses being locked out of their own systems unless they pay a ransom. These attacks can be devastating, leading to operational downtime and significant financial loss. **The FBI reports that ransomware increased by 253% in 2023, targeting businesses of all sizes.**

Insider Threats

Employees, contractors, or business partners with access to company data can pose significant risks, whether due to negligence or malicious intent. **Insider threat incidents increased by 44% in recent years, according to the Ponemon Institute, costing businesses an average of $15.38 million per incident.**

It's not if you are attacked, but when.

Endpoint Detection and Response (EDR)

By focusing primarily on endpoint security, EDR lacks the capability to monitor broader network activity and detect lateral movement within cloud environments, leaving cloud-reliant businesses exposed to attack. While EDR is effective at detecting ransomware on individual devices, it falls short when attacks originate from stolen credentials—a critical weakness given that, according to *Microsoft's Digital Defense Report 2023*, **over 60% of breaches involved credential-based attacks**. Without the ability to assess context, such as unauthorized access via compromised passwords, EDR can allow these types of threats to bypass detection entirely.

Security Information and Event Management (SIEM)

SIEMs collect vast amounts of data, but the time required to manage and analyze this information makes detection slow and largely reactive. Their focus on post-event analysis allows threats to cause significant damage before being addressed.

Additionally, the sheer volume of data can obscure subtle signs of sophisticated or evolving threats, increasing the risk of advanced attacks slipping through unnoticed. Effective defense requires more focused, real-time analysis to stay ahead of these complex threats.

Traditional methods won't provide the coverage needed to remain operational when faced with a threat.

Stop advanced threats at the perimeter with Cloud MDR

What is Managed Detection and Response (MDR)?

Managed Detection and Response is a cybersecurity service that takes protection up a level by combining advanced technologies with human expertise to detect, analyze and respond to cyber threats in real time. Unlike traditional security solutions, MDR is fully managed by a team of professionals, ensuring rapid threat isolation and highly effective threat neutralization for superior protection.

What is Cloud MDR?

Cloud MDR extends the powerful capabilities of MDR to cloud environments such as Microsoft 365 and Google Workspace. As more businesses move to the cloud, MDR must evolve to address the unique security challenges posed by cloud infrastructures, applications, and services. By bringing MDR to the cloud, organizations gain critical protection for identity and access management—key areas frequently exploited by today's cybercriminals.

How does Cloud MDR work to protect your business?

1. Continuous Monitoring

Continually monitoring cloud environments, infrastructure, applications and user activity for signs of abnormal or malicious behavior.

2. Proactive Threat Hunting

Experts are looking for hidden or emerging threats within cloud environments before they can cause damage.

3. Threat Detection

Using a mix of technology-driven and human expertise, to identify threats like phishing attacks, unauthorized access, cloud misconfigurations, or lateral movement within cloud systems.

4. Incident Response

When a threat is detected, a team of experts respond immediately with investigation, isolation and neutralization to minimize the blast radius and prevent further attack.

5. Cloud Specific Security

Tailored to identify cloud-specific vulnerabilities like credential theft and suspicious access behaviors, Cloud MDR surpasses endpoint protection by looking at the context within cloud environments to determine threat.

6. Compliance and Reporting

Cloud MDR assists with maintaining regulatory compliance by providing information and reports needed to adhere to various common compliance frameworks.

Threats are Evolving but Cloud MDR Keeps You One Step Ahead

With Cloud MDR protecting your business, you can be sure that your modern cloud infrastructure enables your business to operate confidently knowing you are protected from end to end. Cloud MDR is the protection of today and is built for the threats of tomorrow.

Contact us for more details.

bwingard@onvetrix.com | www.onvetrix.com | (903) 230-0900

The Benefits of Cloud MDR

- CLOUD TAILORED EXPERTISE
- CUSTOMER TRUST
- DATA PROTECTION
- PROTECTION FROM NEW THREATS
- FASTER THREAT DETECTION & RESPONSE
- SCALABILITY
- ENHANCED COMPLIANCE
- SECURE REMOTE WORK
- REDUCED DOWNTIME IF BREACHED
- REPUTATION PROTECTION