The Ransomware Prevention Guide For SMBs

10 ways to prevent ransomware, with the resources and staff that you have today

Blumira

Blumira.com

Ransomware Prevention Guide for SMBs

Ransomware has officially metastasized into a national security threat. It's estimated that a ransomware attack occurs every 14 seconds.

Small and medium-sized businesses (SMBs) are often ill-prepared to deal with the impact of ransomware and have limited resources to detect and prevent an attack.

Members of small IT and security teams are often responsible for a variety of tasks, from responding to helpdesk and support tickets to maintaining compliance to managing systems and applications. Adding security to that list is often viewed as just another box to check off.

But SMBs need to prioritize ransomware prevention, as ransomware grows in both prevalence and magnitude. In this white paper, learn techniques to prevent ransomware — even with limited budgets and staff.

In this guide, you'll learn

- Specific challenges that SMBs must contend with when it comes to ransomware prevention
- 10 low-cost techniques to gain visibility into your environment and prevent ransomware attacks
- Warning signs of ransomware to look out for
- The true cost of ransomware, taking into account factors such as downtime, legal fees and more
- How ransomware has evolved into a professional, profit-driven market

SECTIONS

01 Introduction
02 Why Should SMBs Worry About Ransomware?
03 Ransomware Challenges for SMBs
04 Ransomware Prevention for SMBs
05 How Blumira Can Help SMBs

Why Should SMBs Worry About Ransomware?

If you're a member of an IT or security team for an SMB, you may be wondering, Why should we worry about ransomware? Ransomware gangs target large, wealthy enterprises. Compared to those companies, we're small potatoes.

Today's ransomware victims aren't companies with extremely sensitive data or Fortune 500 enterprise-level corporations. That's largely due to an emerging industry called ransomware-as-a-service, in which ransomware developers sell malicious code to affiliates. This underground market makes ransomware more accessible to less sophisticated cybercriminals that wouldn't otherwise have the means to launch an attack.

Ransomware-as-a-service has resulted in threat actors taking an approach to ransomware that's purely opportunistic rather than targeted. Threat actors launch ransomware attacks against companies of all shapes and sizes, from every industry.

The ransomware market has also evolved into a professional, profit-driven business operation. Some ransomware attackers even have a "customer support team" that advises victims on how to purchase cryptocurrency to pay the ransom or offers immunity packages to ensure that victims won't get hit twice.

And like any profitable business, ransomware threat actors will likely sink money back into areas of the business that promote growth, such as research and development, to create more sophisticated tools to make money and improve their intrusion tradecraft — which means that simply deploying a firewall and antivirus software and hoping for the best will no longer cut it.

All of this points to the idea that today's typical ransomware victim is simply any organization with a weak enough security posture.

So yes, you should absolutely be worried about ransomware — especially if you're on an IT team for an SMB.

Ransomware Challenges For SMBs

Among malware threats, ransomware is the number one threat to SMBs, according to a Datto study.

SMBs often lack the resources of larger organizations — whether those resources are in the form of personnel, finances, or information. 74% of SMB respondents in a Ponemon Institute study reported that they didn't have the personnel to mitigate cyberattacks; 55% reported that they didn't have the budget to do so, and 47% didn't have sufficient understanding.

In a time when ransomware is so prevalent, IT teams need to prioritize cybersecurity — not treat it like a cost center or an afterthought. Typically, that's a challenge for small IT or security teams that are already responsible for so many other IT tasks. Ransomware is now a business problem, not just an IT problem.

Limited Resources

SMBs often lack the resources of larger organizations — whether those resources are in the form of personnel, finances, or information. 74% of SMB respondents in a Ponemon Institute study reported that they didn't have the personnel to mitigate cyberattacks; 55% reported that they didn't have the budget to do so, and 47% didn't have sufficient understanding.

Limited resources make it difficult to prevent ransomware, but it makes it difficult to recover from a ransomware attack, too. Compared to large enterprises that can afford to pay millions in ransom, SMBs are disproportionately affected by ransomware attacks. 60% of small businesses close within 6 months of being hacked.

74% of SMBs don't have the **personnel** to prevent ransomware attacks

55% don't have the **budget** to prevent ransomware

47% don't have the **understanding** to prevent ransomware attacks

Cloud Services Open Doors to Ransomware

Before the pandemic, SMBs had already started to embrace cloud services, with 59% of respondents using cloud-based apps in a study by SMB Group. During the pandemic, cloud adoption increased by 14% among SMBs as they adapted to new demands and the proliferation of remote work.

Although cloud services help SMBs adapt to post-pandemic work, they also present prime opportunities for cybercriminals. Moving to the cloud often introduces security blind spots, thanks to more complex identity and access management (IAM) and a higher risk of accidental data exposure. In cloud environments, ransomware was deployed 3 times more than any other type of malware.

Cloud is inherently risky, but it's even riskier for SMBs without the resources to secure those environments. 29% of SMBs said they suffered from a data breach after moving to the cloud, according to a report by IS Decisions. The same report revealed that 31% of SMBs found it more challenging to detect unauthorized access since moving to the cloud.

Cloud services also offer a false sense of security. Cloud doesn't inherently equal secure and compliant — even when it comes to the 'big three' cloud providers: AWS, Azure and Google. All public cloud providers operate on a shared responsibility model in which cloud providers are responsible for the security of their own data centers, cloud network, and the hypervisor that creates and runs the host machine. Everything else is up to the public cloud customer.

However, 80% of SMBs simply rely on the native security of the cloud provider.

Hybrid cloud can add even more complexity, as IT teams struggle to get visibility across multiple cloud environments. 56% of SMBs said that they struggled to manage the security of data in hybrid cloud infrastructures.

The True Cost of Ransomware

The actual ransom is only a fraction of the cost of a ransomware attack. Several factors come into play:

DOWNTIME

Downtime and disrupted business operations means a loss in revenue, especially for companies without a disaster recovery plan. **Downtime costs related to ransomware are on average nearly 50 times greater than the ransom, according to a Datto study.**

DAMAGE TO REPUTATION

A ransomware attack can make customers feel uneasy, leading to damaged reputation, and subsequently, customer churn. **86% of people are less likely to deal with companies that experienced a data breach, according to a Semafone study.**

CUSTOMER COMMUNICATION

Companies must follow up with their affected customers after a ransomware attack, and cover costs related to credit monitoring and identity protection services.

LEGAL COSTS

If customer data was breached as a result of the ransomware attack, then companies must incur legal costs related to third-party claims.

REMEDIATION

Remediation costs include implementing forensics and investigative work, as well as containing the actual breach. **Remediation costs grew from an average of $761,106 in 2020 to $1.85 million in 2021, according to Sophos.**

COMPLIANCE FEES

Paying a ransom could breach OFAC regulations and result in needing to pay compliance fees on top of that ransom.

WHAT'S THE TOTAL?

The average cost of ransomware is $4.4 million, according to a Ponemon study.

The same study found that organizations can save $1.12 million on average if they are able to detect and contain a breach in less than 200 days.

That's why the cost of ransomware far outweighs a cloud SIEM investment.

How SMBs Can Prevent Ransomware

Preventing ransomware can seem like a daunting task for SMBs. At its core, ransomware prevention is about achieving visibility into an environment, knowing the stages of an attack, and then recognizing the behaviors associated with those stages.

SMBs should consider these low-cost, effective solutions to mitigate the risk of ransomware.

1. Disable RDP Along Perimeter Devices

Remote Desktop Protocol (RDP) compromise continues to be a top attack vector among victimized companies of all sizes. Windows remote management is enabled by default for many server roles, with little more than single factor authentications and sparse Windows log monitoring.

2. Monitor for RDP Access

To get even more protection against RDP threats, security teams can also use a threat detection and response solution to monitor for RDP access or other risky connections from the internet. Blumira, for example, has a variety of detections that focus on risky connections from the internet, including access to RDP from a public IP.

3. Patch VPN Servers

Software vulnerabilities found in public-facing networking products, such as VPNs, regularly make headlines due to their popularity as attack vectors against SMBs. Similar to exposed RDP, ransomware attackers use these perimeter devices to gain initial network access, escalate privileges and perform lateral movement. It's also critical to remove deprecated VPN products and their associated credentials from the production environment.

4. Deploy Honeypots

A honeypot is a low-cost method to strengthen the defensive cybersecurity of an organization by alerting the security team about an attacker's presence. Honeypots are commonly used by large enterprises and researchers, but they can incredibly useful for SMBs, too.

First, it's important to differentiate between types of honeypots. Research honeypots — virtual systems with vulnerable operating systems that are deployed on an Internet-accessible network — are time-consuming to set up and maintain. However, production honeypots emulate a high-value item, such as a workstation, document, or web server, and are low-interaction systems. These are particularly useful for time-strapped security admins that can take a 'set it and forget it' approach and let the alerts roll in.

Free, open-source honeypots include Thug, Honeydrive and Dionea, but the caveat is that they will require some legwork to set up and maintain. Other options include Blumira's virtual honeypot, which enables simple deployment with the click of a button.

Once deployed, honeypots can monitor for indicators of a ransomware attack, such as lateral movement, password spraying and network sweeps carried out by similar IP addresses.

Learn more about Blumira honeypots ->

5. Enable Sysmon

When it comes to preventing ransomware, it's important to have visibility into an environment. Endpoint detection and response (EDR) tools can achieve that, but they can also be expensive and out of the question for smaller companies with limited budgets.

System Monitor (Sysmon for short) is a free Microsoft utility that small IT teams can use to get visibility into their environments. Sysmon is part of the Sysinternals software package and provides a higher level of event monitoring than the standard Windows logs. It records events such as network connections, process creations, file hashes, and changes to the Windows Registry. At a minimum, SMBs without the budget for an EDR solution should deploy Sysmon for enhanced logging that can provide a wealth of data about company endpoints.

Since Sysmon is free, it does require more care and feeding than a plug-and-play paid tool. IT must deploy updates as they are released and make configuration changes as necessary, but those tasks generally fall under the umbrella of standard patch management. Installing and configuring Sysmon is relatively easy and can be achieved in a few steps.

Check out Blumira's guide to configuring Sysmon->

6. Centralize Logs

Deploying Sysmon is a good first step for IT and security teams, but without centralizing those logs, they won't get the full value from it. Sysmon by itself doesn't generate alerts; it simply logs events. Only logging the endpoints themselves will be good for incident response, or knowing exactly what happened after the fact. But pulling the logs into a centralized platform will give IT and security teams more immediate alerting that will be critical for detecting and preventing security incidents.

An open-source centralized log management tool like NXLog is a solid option for SMBs. Blumira offers a free tool, Flowmira, to extend the capabilities of NXLog. Flowmira is a set of customized NXLog configurations that IT admins can use to generate data from Windows endpoints.

Learn more about using Flowmira with NXLog>

7. Deploy Threat Detection & Response

Using Sysmon and a centralized log management tool will provide some visibility into an environment and help with alerting, but small IT and security teams need to know how to respond to those alerts. A threat detection and response solution like Blumira alerts IT and security teams on suspicious behavior that is indicative of a ransomware attack, but also gives steps for remediation through in-depth security playbooks. Blumira also comes with security experts that will give guidance on next steps and act as trusted partners in a security program.

8. Prioritize Both Offline and Online Backups

If a ransomware attack strikes, the best way to avoid major financial damage is to restore the encrypted data from clean backups. Businesses that restore from a backup can typically avoid paying the ransom, which is an expensive and often unreliable method of getting data back.

Most organizations will have some sort of backup solution, but for SMBs, that sometimes takes the form of an onsite local storage backup solution that stays plugged in. Unfortunately, ransomware threat actors will take note of onsite storage and target it as a part of the attack.

To prevent this, SMBs should run two forms of backup at minimum and at least one of those should be offsite. Other best practices include performing online backups on a weekly basis and offline backups on a monthly basis, at minimum. IT and security teams should also test backups to ensure that they're able to recover systems and data in the event of an attack.

9. Know The Early Warning Signs

The best way to prevent ransomware is to detect and stop an attack in its early stages. However, nearly half of SMBs don’t have the knowledge or understanding to prevent an attack, according to the aforementioned Ponemon Institute study. IT and security teams should familiarize themselves with common early-stage warning signs of a ransomware attack, such as the emergence of network scanners, MimiKatz, and Microsoft Process Explorer.

> *“We don’t have dedicated people to just sit and wait for things to happen. Our team has to split their time to support various systems and projects. Everyone on the team plays a key role in our security. Getting responsive alerts is important so we can respond quickly to potential risks.”*
>
> – **Angela Bawcum,** Interim Director of IT & Infosec,
> Lawrence Technological University

10. Teach End Users About Phishing

IT and security teams should know about ransomware warning signs, but so should end users. Phishing emails that look legitimate but are embedded with malicious links or attachments are often the first step of a ransomware attack. At a minimum, IT and security teams should inform end users about how to spot a phishing email. More formal security awareness training is even better, but an informal chat about what a phishing email can look like and what to do is a good first step for SMBs.

6 Warning Signs of Ransomware

Ransomware can create major damage. Stop ransomware in its tracks by knowing the warning signs.

1 Suspicious Emails

Ransomware attacks often starts with a phishing campaign. Attackers send emails that may look legitimate, but are embedded with malicious links or attachments.

2 Network Scanners

The emergence of network scanners - especially on servers - could be inconsequential, but it could also be the sign of cybercriminals attempting to infiltrate your network.

3 Active Directory Access

Hackers often use tools such as BloodHound and AD Find to infiltrate Active Directory and gain domain access.

4 MimiKatz and Microsoft Process Explorer

Cybercriminals often use MimiKatz and Microsoft Process Explorer to steal credentials. The presence of MimiKatz should always be a red flag.

5 Software Removal

Software removal programs like Process Hacker and GMER can be a sign of cybercriminals attempting to remove security software, like antivirus.

6 Small-Scale Test Attacks

Hackers will sometimes perform dry runs to find any vulnerablilities in your network before they deploy a full-scale ransomware attack.

Blumira

How Blumira Helps SMBs Prevent Ransomware

Preconfigured so you don't need a security team to run it

Blumira acts as an affordable replacement for a security operations center (SOC) that's attainable for smaller, resource-strapped IT and security teams. Blumira protects SMBs against ransomware by alerting teams about the indicators of a ransomware attack, such as password spraying, network scanning and unauthorized RDP access. Blumira detects these behaviors and more, sending prioritized alerts about a ransomware attack early in its stages to prevent infection.

One of the challenges for SMBs is a lack of knowledge about how to prevent ransomware. Blumira solves that challenge by providing contextual alerts and a dedicated team of security analysts that can provide advice on how to remediate, which helps to not only prevent risks but build a stronger security culture in the long term.

Blumira's security playbooks will guide teams through best security practices and next steps to reduce their overall attack surface.

The Blumira Platform is Preconfigured to:

Collect and Centralize Security Events

Applications and security tools across your environment connect with Blumira's virtual sensor to collect and stream security events, logs and alerts straight to Blumira's cloud service.

Provide Guided and Actionable Remediation Playbooks

Guided and actionable remediation playbooks enable any member of your organization to easily respond and stop the security threat, even when the responder might not have security expertise.

Rapidly Detect Cybersecurity Threats

Backend automation and fine-tuned alerting increase the effectiveness of threat detection while reducing the noise of false-positive alerts. Virtual Honeypot(s) are deployed with the click of a button to detect lateral movement across your environment.

Automate Remediation

When known cybersecurity threats are detected, automated remediation capabilities can implement blocking rules to stop active threats without manual intervention.

> “I like that [Blumira] not only provides good details on findings, but also suggestions on what to do about them. With our previous solution, it would often be 24 hours before we would receive alerts from our partner and we had to do a lot of manual analysis.”
>
> – **Bryan Allen**, Sr. Systems Analyst, Lawrence Technological University

Security threats are constantly evolving and traditional SIEMs are unable to keep pace. Unscalable solutions that require immense effort from expensive teams of security experts prevent even the largest of enterprises from achieving a robust cybersecurity program. When assessing which SIEM product to choose for your organization, it is crucial to understand each solutions’ deployment and configuration options, the extent to which it automates threat detection, if it provides playbooks for remediation, and whether or not its’ reporting is comprehensive enough for your needs.

Blumira’s cloud-based easy-to-use platform provides an all-in-one tool to effectively protect your organization from evolving and new security risks without the need to hire an expensive team. Our mission is to provide affordable, comprehensive security solutions to organizations of all sizes -- without complication or overhead.

Sign Up For Your Free Account

Get your free account with Blumira and secure your Microsoft 365 environment in minutes. No credit card required.

Sign Up Free