BLUE RIDGE® NETWORKS

Guard Government Services from Ransomware Attacks

Ditch the Fire Drill with a Zero-Trust Approach

WHITE PAPER

Table of Contents

Summary

Ransomware attacks are on the rise and they are bringing state, local, and municipal governments to their knees, grinding services to a halt and disrupting revenue collection. With departments being forced to switch from online to manual offline processes, efficiency and productivity also suffers.

As ransomware tools and methods evolve and adversaries skills grow with each attack, government agencies are finding themselves increasingly targeted by attackers. As providers of essential services, government agencies can ill afford the downtime and the cost associated with remediation.

Furthermore, under-resourced security teams and un-hardened systems expose government networks, many of which aren't sufficiently locked down to survive a ransomware attack. Meanwhile, conventional endpoint solutions like antivirus and intrusion detection either can't or don't stop an attack, leaving security teams in a reactive, fire drill mode.

In this paper, we'll:

- Discuss the challenges that government agencies face in managing the ransomware threat.
- Consider the consequences of doing nothing or relying on traditional approaches.
- Introduce a cost-saving, low-overhead solution that guards systems from attack by disrupting the earliest and subsequent stages of ransomware attacks that are undetectable by other endpoint cybersecurity approaches.

The city has already spent $2.6 million recovering from a ransomware attack that demanded a roughly $51,000 payment.[1]

Cities Held for Ransom

Shockwaves reverberated across the state and local government community in March 2018, when the city of Atlanta was ground to a halt by a ransomware attack. City officials spent two weeks restoring online internal systems and citizen-facing application services disrupted during the attack, yet many services remained offline beyond that time.

Below are just some of the casualties:

- The Department of Finance couldn't issue business licenses through its web page.
- The Atlanta Municipal Court was unable to process ticket payments.
- The Department of Watershed Management was unable to accept online water and sewer emergency service requests.
- The Department of Parks and Recreation had to manually review permits and event applications.
- Applications for new employment were suspended.
- Two services were taken down voluntarily as a precaution: the Hartsfield-Jackson Atlanta International Airport wi-fi network and the ability to process service requests via the city's 311 web portal.

Atlanta now joins an unenviable club of governments and organizations that have been victims of high profile ransomware attacks. Though the concept of holding data hostage for a ransom has been around for almost a decade, 2017 saw a surge in activity with Symantec noting in its 2018 Internet Security Threat Report that "ransomware criminals have been busy adding more strings to their bow" including new tools and targets.[2] Symantec detected approximately 1,242 average ransomware infarctions (including the notorious WannaCry) each day in 2017, while McAfee saw a 59% increase in ransomware in the same year.[3]

The Current State of Ransomware

Ransomware is a form of malware commonly delivered as highly targeted phishing emails and masquerading as a file that users should trust. Once downloaded and opened, the malware takes over the computer or network. It then blocks or encrypts access to data, files, and even systems, and demands a ransom to restore access.

Ransomware has reached a critical peak, for several reasons:

- **Ransomware is evolving.** For example, the SamSam ransomware strain that impacted Atlanta infiltrates networks, not through phishing or online scams, but by exploiting vulnerabilities (such as unpatched server-side software) or guessing weak passwords in the target's public facing systems. Once in it uses the popular password discovery tools, such as Mimikatz, can then be used to gain control of the network. SamSam has been adapted to exploit a variety of vulnerabilities in remote desktop protocols, Java-based web servers, File Transfer Protocol servers, and other public network components.
- **Ransomware has also become a commodity.** Ransomware thieves don't have to be tech-savvy anymore; commercial malware kits can be purchased by any criminal on the dark web.
- **Data backups can't protect you.** Many organizations assume that data backups are a solution to the problem. However, incomplete backups and those that skip certain endpoints, such as mobile devices or remote workers, don't cover all bases. Furthermore, new ransomware variants can attack unmapped networks and cloud-stored assets that aren't included in typical backup instances. Some even target backup files themselves.
- **Ransomware is attracting new threat actors.** Once the preserve of cyber criminals, new data suggests that targeted attack groups, attracted by the disruptive capabilities of ransomware as well as the lucrative profits, are entering the fray. WannaCry, for example, which first made headlines in 2017, was assumed to be the work of cyber criminals but the FBI has since linked it to the North Korean regime.

Why State and Local Government is Such an Attractive Target

It's not that the government is more susceptible to these types of attacks than the private sector, but that they're a bigger target. Government systems must be accessible to the public, for instance, to pay fees or find information. These public-facing networks must be better protected so that vulnerabilities there don't affect more sensitive information on other systems.

The Atlanta attack was carefully chosen. Local governments, as well as hospitals and health record firms, education institutions, and industrial control services, are more likely to pay the ransom rather than risk extended downtime. Ransoms are set a price point that is perceived as manageable for such organizations.

And while Atlanta's critical law enforcement and public safety teams were spared the attack, The Hill reports that there have been 184 attacks against public safety agencies in the last 24 months.[3] Critical to public safety and the community, attackers hope they are more likely to pay. But that's not always the case; many government victims of ransomware don't pay the ransom, yet the outcomes are still costly:

- In November 2017, **the San Francisco Municipal Transportation Agency (SFMTA),** which operates the MUNI light rail system, was attacked by ransomware. While the ransomware did not penetrate the agency's network, it did shut down ticket vending machines. Hackers demanded $70,000 in Bitcoin. To prevent disruption in service, SF Muni offered free rides until the fare machines were operational again. The agency did not pay the ransom, but the attack was very costly.

- In February 2017, **the city of Los Angeles Integrated Security Operations Center (ISOC)** identified 16 ransomware attacks in five city departments. The attacks were segmented, no data was lost, and no ransom was paid. In an effort to stay one step ahead of future attacks, the city is budgeting $2.25 million in funding to support cybersecurity initiatives.

- In August 2016, **the city of Sarasota in Florida** had a ransomware attack that shut its computer systems down by a type of ransomware that entered the city's system through a virus that was sent to one employee. Despite demands by hackers, the city did not pay the ransom and was finally able to recover its files. The cost of resources, lost productivity and inability to provide services, however, was very high.

Whether city officials pay the ransom or not, the cost of ransomware is significant – disruption of services, loss of revenue, and loss of public confidence.

The big takeaway here is the growing trend that criminals and targeted attack groups are directly targeting government organizations in ransomware attacks. Attacks like Atlanta will happen again.

Challenges of Current Approach: Government is Stuck in a Reactive, Fire Drill Mentality

Despite best efforts, many government networks aren't sufficiently locked down to survive a ransomware attack. A lack of resources and poor cyber hygiene is an ongoing problem that even big cities like Atlanta struggle with. Wired reports that a City Auditor's Office report from January 2018 shows that the City of Atlanta recently failed a security compliance assessment. A lack of formal processes to identify, assess, and mitigate risks means that even deployed security controls are ad hoc or undocumented, "at least in part due to a lack of resources."[5]

Atlanta isn't alone. Many municipalities have a limited IT budget, often operating with a security team of one. Without proper resources, implementing standard security practices can be challenging. 59% of government security personnel say their agency struggles to understand how cyber attackers could breach their systems. Furthermore, 65% don't think the government can detect ongoing cyber attackers.[6]

Municipalities need a simple, less complex and resource-intensive solution to their security challenges. While government and industry cybersecurity experts have advocated hardening systems with continuous monitoring, intrusion detection technology and patch management, these approaches invite the sort of reactive fire drill mentality we see again and again. A key challenge for government agencies is that these conventional endpoint cybersecurity solutions either can't or don't stop an attack, rather they attempt to detect or contain a compromise that has already occurred, then attempt to respond in sufficient time to limit its effects.

Prevention, Not Detection: The AppGuard Difference

Rather than focus on the detection of ransomware and other forms of malware, industry experts stress an emphasis on prevention. A zero-trust stance would help agencies proactively secure their endpoints and networks because it assumes everything on their systems is already compromised and blocks unacceptable actions.

With its a unique, patented, multi-layer endpoint defense, AppGuard prevents breaches from occurring by disrupting the earliest and subsequent stages of ransomware attacks that are undetectable by other endpoint cybersecurity approaches.

For example, ransomware generally manifests itself through a drive-by download attack from a web browser or an email attachment. AppGuard prevents these attacks from running, and is effective in stopping phishing attacks, data theft, ID theft, and many other types of prevalent threats.

> ***"AppGuard should be on every Windows system in the world."***
>
> – Robert Bigman, Former CISO, CIA

How is this approach different to antivirus? Traditional antivirus software relies upon signatures and then scanning to identify malware and ransomware, but signature-based approaches cannot defend against malware until samples of the virus are obtained, signatures generated, and updates distributed to users – making them ineffective against new emerging undetectable malware attacks. That is why signature-based approaches are not effective against zero-day malware.

AppGuard prevents ransomware from detonating without requiring signature-based detection, scanning, or updates, thus preventing compromises from occurring. It delivers valuable Indicators of Attack (IOA) well in advance of conventional detection, response, and containment products which typically rely on detecting and identifying Indicators of Compromise (IOC) after a compromise has already occurred.

By design, AppGuard assumes that endpoint applications have unknown exploitable vulnerabilities, hence, the name – AppGuard. The solution's controls effectively place these applications under "guard" so they can do no harm. AppGuard blocks attacks on endpoints without having to recognize the malicious code or ever-changing details of the endpoint's applications. It not only adapts automatically to application updates, but it also compensates for missing security patches, freeing limited resources to do other important tasks. Patching is still prudent. But it does not need to be rushed or done at the expense of other important tasks and can be verified prior to deployment.

The good thing is that AppGuard is designed to be compatible with most popular antivirus tools which can still be useful for performing system maintenance from time to time to remove unwanted code rendered dormant by AppGuard.

True Set and Forget Endpoint Protection

By preventing endpoint compromises without signatures of any kind, AppGuard requires no updates or help from the cloud to protect endpoints from the latest threats. Antivirus and machine learning products require continuous updates and their detection rates decline when offline. AppGuard even protects offline endpoints ranging from end-users viewing email attachments on airplanes to industrial control systems and other special function endpoints that must be isolated from the Internet and normal IT space.

Stop Known and Unknown Threats

AppGuard is designed to stop both known and unknown malware from making its way onto your computer.

AppGuard has the capability to essentially prevent breaches - call it instant response without detection - for any of these forms of new malware.

Nip Cyber Costs at the Endpoint

The failure of antivirus protection at the endpoint has been driving up the data breach volume, increasing the costs required to prevent, detect, and respond to them. These costs manifest in the forms of tools, services, personnel, business processes, and readiness exercises for areas such as: cyber hygiene, security incident and event management (SIEM), next generation firewall, breach detection system (BDS), incident response, forensics, remediation, threat intelligence, and operations optimization. Endpoint incident/alert volume directly relates to all these downstream costs. AppGuard nips these costs in the endpoint.

Alleviate the Cyber Skills Gap

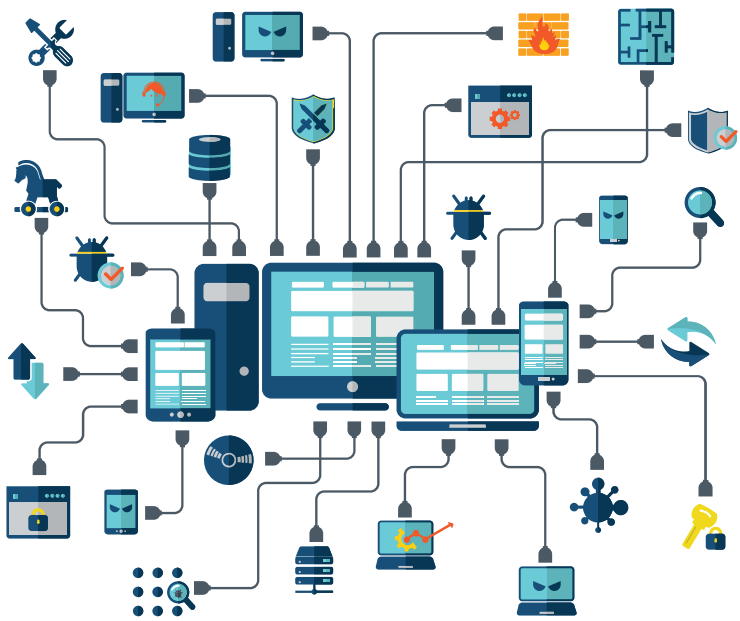
AppGuard requires no special expertise to administer; it's designed for Windows administrators. Editing policies are as simple as adding a song to a playlist. Because AppGuard simply blocks unacceptable actions, administrators are not put in the position of having to analyze and react to alerts as is required of EDR and some post-execution products.

Furthermore, AppGuard alleviates the pervasive cyber skills gap and lack of cyber resources in municipal government in two ways. First, it doesn't require highly skilled IT professionals to protect endpoints. Second, its highly effective protection reduces all forms of incident/alert volume downstream from potentially compromised endpoints. Most organizations, which lack AppGuard-like endpoint protection, have deployed many different cyber functions that require constant monitoring, interpreting, and reacting to alerts.

How AppGuard Excels Over Sandboxing

Traditional breach detection systems use sandboxing techniques have their usefulness, but they can interfere with user productivity and introduce the possibility that a user may be operating in a compromised sandbox. In contrast, AppGuard employs dynamic containers in conjunction with its micro-isolation technology.

Any application can be added to AppGuard's robust default containment group which AppGuard will automatically protect. Attacks are halted at the first stage, so there's no need to worry about compromised user workspace or system resources. Plus, "sandboxing" is largely ineffective for addressing emerging advance threats such as spear phishing, watering hole, or advertising attacks, where AppGuard excels.



Defeat More than Just Ransomware

In addition to ransomware, AppGuard defeats consumer malware, advanced malware, exploit-less (e.g., PowerShell or other scripts that use legitimate utilities to do harm), and file-less (reside in memory only) attacks on endpoints. It does so by avoiding the dilemma of telling good from bad files or normal from abnormal behaviors amongst infinite, transient possibilities. That's why alternatives fail and incur high operational costs.

Instead, AppGuard's patented approach uniquely blends low-level controls that dynamically block unacceptable yet deterministic actions. Adversaries can easily change how malicious code looks and behaves but changing what it ultimately does without sacrificing their goals is extremely rare. Endpoint attackers cannot achieve their goals without successfully executing these finite actions.

Experience Ransomware Protection: "As a Managed Service"

AppGuard is ideal for resource-constrained municipal agencies. With the option of a fully-managed service, once installed, no user interaction is required. AppGuard works to protect against ransomware, completely autonomously.

The solution also eliminates the tedium of security patching. AppGuard does not require constant updates or lists of known, it builds lists of known security threats already identified by other sources. Its integrated software-only approach is seamless with all Microsoft Windows platforms, stands alone with no OS hooks, and includes all documented APIs.

AppGuard is available in two flexible deployment options:

- **AppGuard Enterprise** can be deployed as a fully-managed or co-managed service in the cloud, or as an enterprise site license with essentially no limit to the scalability of the management system and the number of endpoints it can manage.

- **AppGuard Business** delivers an affordable solution for small and mid-sized organizations to comprehensively protect their systems and operations without complexity or overhead.

AppGuard – "Futureproof" Breach Prevention for Government

AppGuard delivers a breakthrough ability to prevent breaches on endpoints from emerging advanced threats that conventional cybersecurity approaches cannot address.

People and organizations all over the world are ever more interconnected via the endpoint devices in their lives. AppGuard delivers simple, effective, affordable solutions to the complex security challenges that threaten the interests of government organizations and their constituents.

AppGuard is the only security product in the marketplace that is currently undefeated by any kind of ransomware and malware and it deploys a unique methodology to achieve this.

- **No endpoint protected by AppGuard has ever been breached.**
- **AppGuard is more effective than traditional EDR and antivirus solutions.**
- **No sandboxing or cumbersome processes are involved.**
- **It has the lightest footprint in the industry if only 1MB.**
- **It scales to over 100,000 endpoints and provides a central management architecture that is simple, elegant, and cloud efficient.**

That is why security experts and analysts recommend that enterprises supplement their endpoint protection platform with advanced protection agents such as AppGuard.

> ***"For over 2 years, AppGuard has been a cost-efficient and effective endpoint protection solution that made our network more secure."***
>
> – Ian Gottesman, CIO, Center for Strategic and International Studies (CSIS)

References

1. https://gcn.com/articles/2018/04/24/costs-atlanta-ransomware.aspx
2. https://www.symantec.com/security-center/threat-report
3. https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2018.pdf
4. http://thehill.com/opinion/cybersecurity/381594-a-ransomware-attack-brought-atlanta-to-its-knees-and-no-one-seems-to
5. https://assets.kpmg.com/content/dam/kpmg/pa/pdf/federal-cyber-survey-2016.pdf
6. https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/

About Blue Ridge Networks

Based in Northern Virginia, Blue Ridge Networks is a visionary cybersecurity pioneer that provides autonomous cybersecurity for the connected world. Blue Ridge Networks' Autonomous Cybersecurity Suite protects organizations from vulnerabilities posed by connected devices, endpoints, networks, and people. Blue Ridge solutions have protected critical operations for some of the largest US government, financial, healthcare, and other critical infrastructure customers for more than twenty years with no reported breaches.

Contact Us:
1-800-722-1168
sales@blueridgenetworks.com

Headquarters:
14120 Parke Long Court Suite 103
Chantilly VA, 20151