# Prevention and Detection: How to Build a Layered IT Security Program that Works

We all know that an ounce of prevention is worth a pound of cure. This guide will help you to understand the different layers of IT security and how you can prevent most security breaches - and detect the exploits that still get through.

BUFFERZONE

# Introduction

"Security is always excessive until it's not enough." Sage words from the head of security of a public utility company. Certainly when it comes to information security in this day and age, "excessive" isn't even in the lexicon of those who are responsible for securing their organization's computer systems and information assets.
The question is, what is "enough"?

Building, implementing and maintaining a comprehensive computer security program is quite a challenge for any organization, but especially so for small and medium-sized businesses (SMBs) with limited budgets and small IT and security staffs. Nevertheless, it's an absolute necessity. If your organization doesn't have a strong IT security program, you're playing a risky version of Russian roulette, and the chamber is loaded with bullets.

By isolating and snuffing out attacks as they enter your environment, you can vastly improve your risk posture and give your employees the latitude to work without fear of allowing malware into the company.

What makes the situation so risky today? By and large, it's because the threat landscape has radically changed and it continues to morph as time goes on. Practically every genuine business entity with an Internet connection - regardless of location, size or industry sector - is subject to cyber attacks today. From nation-states to cyber criminals to hacktivists, there are plenty of people with the motivation and the means to target your business.

Cyber attacks now take place on an industrial scale. According to the 2015 Global State of Information Security Survey, the compound annual growth rate of detected security incidents has increased 66% year-over-year since 2009[1] Making matters worse, Trustwave estimates that as many as 71% of compromises go undetected[2] In 2012, cyber attacks on small businesses rose 300% over the previous year-and they've been on the rise ever since[3] The problem is now so acute that more than half of U.S. companies regard the threat from cyber attacks as one of their top three business risks.[4]

As the threat landscape grows more ominous, industry pundits add to the confusion of what to do about it. They proclaim things like "anti-virus is dead!"[5] and "prevention is futile"[6] and this makes it all the harder to know what to do to create a comprehensive security program.

**We're here to help clarify what you should do. This white paper presents an overview of how to develop a layered approach to protecting your most important digital assets, with a focus on what you can do to secure your largest and most vulnerable attack surface. By isolating and snuffing out attacks as they enter your environment, you can vastly improve your risk posture and give your employees the latitude to work without fear of allowing malware and other threats into the company.**

---

[1] PwC, The Global State of Information Security Survey 2015, www.pwc.com/gsiss2015

[2] Trustwave Holdings, 2014 Trustwave Global Security Report, May 2014

[3] Symantec Corporation, Internet Security Threat Report 2013

[4] BAE Systems, Business and the Cyber Threat: The Rise of Digital Criminality, February 201

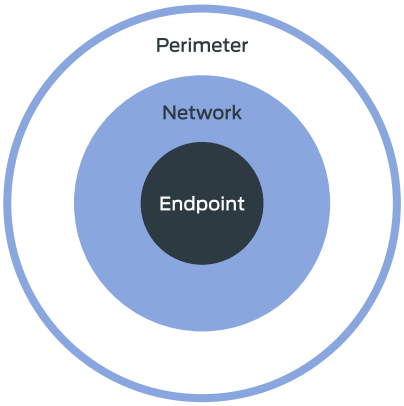
[5] In May 2014, Brian Dye, Symantec Corporation's senior vice president for information security, stated "anti-virus is dead" in an interview with The Wall Street Journal.

[6] Gartner issued a report that says that attack prevention will be futile by the year 2020

# IT Security Must Be Multi-dimensional

Remember the saying when the weather changes in layers so you'll be ready for anything. Well, we're in a business environment today where the cyber threats change rapidly. Attackers have learned to craft their malicious software to evade common detection techniques. Thus the best thing you can do for your business is to dress your computing environment in layers of protection so you'll be ready for anything.

**Protecting in layers means you need to put defensive measures at the points of significant vulnerability - at the endpoints that workers use, on the company network, in cloud storage and applications, and around your sensitive information and data that thieves would want to steal.**




- **At the endpoint** - The devices that workers use to access your company's computer systems and assets are commonly called endpoints. Because there are many of them in use, endpoints - and the people who use them - represent the biggest attack surface your company has. Some attacks that originate at the endpoint are indiscriminate, such as drive-by malware downloads during website browsing, while others are very targeted to a specific individual, as in the case of a spear phishing email. End users themselves can introduce malware with an innocent action like plugging a compromised thumb drive into a USB port, or by using unsecured Wi-Fi at a public place and inadvertently enabling a man-in-the-middle attack. People are vulnerable to social engineering attacks that prey on their trust and encourage them to click on malicious web links or open booby trapped attachments.

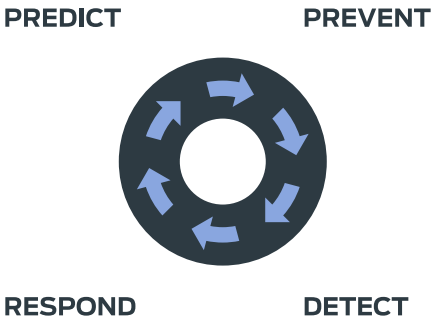
- **On the network** - For companies that have an Internet-facing presence (and what company today doesn't have one?), the network is where attack traffic comes in; for example, via the email server or a network router or gateway. Moreover, this is the level where command and control (C&C) communications go out and data is exfiltrated during a breach. Inside the network, traffic flows laterally from one internal device to another, usually unchecked and uninhibited, and this is how attacks spread once they have a foothold inside your network. Thus it's critically important to deploy security solutions at this major point of vulnerability.

- **In cloud storage and applications** - Most companies today take advantage of using data storage and business applications that are hosted in the cloud, rather than in their own data center. Cloud applications are especially beneficial to SMBs who don't want the hassle and expense of installing and operating their own hardware and software. If your company has important data in the cloud, you need to have proper controls to secure the data and to ensure that only authorized people have access to it.

- **Around data** - Data is what it's all about - it's what you are really trying to protect. Whether data is actually stolen by a cyber thief or accidently exposed by a careless employee, you need to apply protection directly to and around the data to ensure it can't be used if lost, stolen or otherwise exposed.

IT security must be multi-dimensional, which means you need tools for the entire security lifecycle.

- **Prevent** - It's far less expensive to prevent attacks from happening in the first place than to detect and stop them once they are underway. Preventative measures may not stop 100% of attacks but it's absolutely critical to try.




- **Detect** - Try as you might, some threats may get through the preventative defenses, and so it is important to look for signs of an intrusion within your systems. Detection technologies have become very sophisticated and fine-tuned, looking for even the smallest indicators of compromise and correlating them with other bits of information to put them in context and try to determine if an attack is taking or has taken place. Unfortunately, statistics from breach investigations indicate that the gap between the time to compromise a system and the time to detect the compromise is growing larger.

- **Respond** - The sooner you can detect and respond to a confirmed security incident, the less damage you'll have. Of course, if detection of the compromise takes months, the response might well involve breach notification and clean-up.

- **Remediate** - Whether a security incident is discovered right away or months later, there will be some level of remediation necessary, such as reformatting and completely cleansing an infected PC.

Everything we've talked about to this point has been about protecting systems, but it's also important to think about people in this equation. People must be given security awareness training and the responsibility to report suspicious incidents or activities - even if they, themselves, have caused the incidents – to attempt to prevent or at least quickly detect attacks.

**Security has to work in many dimensions. You need all of the layers around systems and people to protect your business today. Let's talk about how to build your IT security program.**

# Start with Prevention

**An ounce of prevention is worth a pound of cure. It's another idiom you've heard all your life that we can apply to IT security. Prevention is by far more cost effective as a security measure than trying to detect when an attacker is already within your systems. Prevention can largely be conducted with automated technology alone and with little intervention by expensive skilled IT security professionals. Detection, on the other hand, not only requires very sophisticated technology that draws data bits from numerous sources but also continuous monitoring and frequent analysis and action on the part of highly skilled information security experts. Moreover, once you are in the detection phase, you might also be experiencing actual damage**

## Secure the Endpoint

Most cyber attacks begin at the endpoint and the person at the device, so your prevention must start here. There are three major classifications of endpoints-traditional PCs, including desktops and notebooks/laptops; client systems in a virtual desktop infrastructure (VDI); and mobile devices such as smart phones and tablets. Of the three classifications, PCs are the largest attack surface today, by far.

### PCs as endpoint devices

The vast majority of desktop and notebook devices run some version of the Microsoft Windows operating system (OS). Because Windows has been architected to allow generous interoperability among different software programs and peripheral devices, PCs are vulnerable to attack.

There are three primary external sources of threats to PCs and the people who use them: insecure web browsers and compromised websites that allow malware to be "dropped" onto PCs are without the users' permission or knowledge; removable media such as USB thumb drives and DVDs; and email messages containing links to compromised websites or attachments with malicious payloads.

Most cyber attacks begin at the endpoint and the person at the device, so prevention must start here. The three primary external sources of threats to PCs and the people who use them are: insecure web browsers and compromised websites that allow malware to be "dropped" onto PCs; removable media containing malicious code; and email messages containing links to compromised websites or attachments with malicious payloads.

The traditional strategy for protecting PCs from these threats is to install anti-virus (AV)/anti-malware software on the endpoints to scan for malicious code. Still commonly used today, this approach largely depends upon comparing suspicious code to "signatures," or code that is known to be malicious. The obvious weakness here is when the suspicious code has no match in the signature file and is then erroneously deemed to be safe. This happens more often than you think. In fact, 83% of current anti-virus solutions would fail to detect the top malaware campaign delivered by spam on any given day. [7]

[7] Malcovery Solutions, Fortify Your Network Protection with Actionable Intelligence using Today's Top Threats, April 2014

In response to the shortcomings of AV software, security vendors have come up with the practice of "sandboxing," or placing suspicious code into a test environment for a short time to allow the code to run to see if it is malicious. It's a good idea with a glaring weakness: malware coders have learned to circumvent sandbox technology by delaying the execution of the malicious code until after it is released from the sandbox.

**The new strategy for protecting PCs from threats is to create a completely isolated environment for all untrusted activity to take place. No malicious code that executes in this environment can cross over to the trusted side of the PC or the network it is on. Thus, if a worker opens an email attachment that contains malware, or clicks a link that leads to a compromised website that drops malware onto the PC, or inserts a thumb drive infected with a virus, all of these activities take place in an isolated "bubble" where they can't cause any harm or spread to other devices. Attachments and other files that don't pose a threat can be safely moved from the isolation environment to the normal work environment so that productivity doesn't suffer.**

**The brilliance of this prevention approach is that it works on unknown malware that has no AV signature yet as well as on previously known malware. What's more, all of this isolation, security testing and transfer of files to a trusted environment happens automatically, in the background, without human intervention and without disrupting worker productivity.**

## Here are some options for security layers on PCs:

- **Anti-virus/Anti-malware software** - This security measure looks for malicious code based on known signatures, pattern matching or behavior matching. Though it's efficacy is low, AV software is still highly recommended as a minimal protective measure for every PC, and is required by many regulatory standards. Consider endpoint protection platforms from vendors such as McAfee or LANDESK.

- **Desktop firewall** - Also called a personal firewall, this software application protects a single Internet-connected computer from intrusions. It works in the background to filter inbound and outbound traffic to protect the integrity of the system from malicious code.

- **Host-based Intrusion Prevention System (HIPS)** - HIPS is an installed software package which monitors a single host PC for suspicious activity by analyzing behavioral events occurring within that host. In case of attempted major changes by a hacker or malware, HIPS blocks the action and alerts the user so an appropriate decision about what to do can be made.

- **Containment** - This is an approach that isolates untrusted applications such as a web browser, email attachment or Skype within a protective container environment, so that malicious code is prevented from crossing over to the regular PC environment. It is nearly transparent to end users but contains both known and unknown threats.

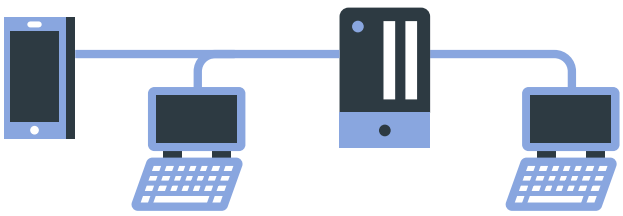
- **Application control** - This is an approach whereby only approved applications are permitted to run on the PC. It blocks all unapproved software from running.
  While this creates a secure environment, it also can be detrimental to worker productivity if they can't run software applications they need.

- **Data Loss Prevention (DLP)** - DLP is software that monitors for specific types of information that are being copied or transferred off the PC or network, and then blocks the action. For example, DLP can watch for data that contains Social Security numbers and prevent it from being exfiltrated.

As you consider your approach(es) to preventative PC security, be mindful of the impact the solution(s) may have on end users. If the security is a hindrance to getting work done, people will find a way to circumvent the measures.

## VDI configurations

In a virtual desktop infrastructure, the endpoint devices are typically "thin client" PCs where the desktop operating system is hosted on a server rather than on the PC. The endpoint device doesn't have any (or much) processing capability on its own; it receives content to be displayed on the thin client from the centralized server. In theory, this is supposed to create a secure endpoint environment, since the endpoint doesn't store or process data or applications. In reality, the vulnerability is transferred from the endpoint devices to the central server that runs the desktop OS for many thin clients.



**Security experts contend that VDI out-of-the-box is in itself not more inherently secure than traditional desktops. It still needs to be complemented with additional security layers, just like a traditional desktop environment [8]. Many of the same solutions that are listed above can solve the security challenges of VDI.**

[8] The Virtualization Practice, A VDI desktop is No More Secure than a Standard Desktop

## Smart phones and tablets as endpoint devices

Mobile devices are a different kind of security challenge. First of all, they are often owned by the user and not by the company, so it's hard for the company to dictate how the device is configured. Many organizations now are using mobile device management (MDM) technologies that manage only the "business side" of the device. Such MDM solutions have the ability to provide some protections, such as policy enforcement, and remote wipe if the device is reported lost or stolen.

An important complement to MDM is NAC, or network access control. NAC is used to ensure that mobile devices, and mobile or remote PCs as well, are compliant with your company's security policies before allowing the device to have complete access to your network. For example, if a device is found to be running an out-of-date version of its operating system, the NAC device can quarantine the endpoint device from the network, and perhaps give it only basic Internet access.

Many workers use their smart phone like a USB thumb drive, plugging it in to their PC to download photos or listen to music. This action introduces several potential concerns: insider theft of corporate data, and transmission of Windows-based malware from the smart phone to the PC. In either case, technologies and policies that treat the smart phone the same as any other USB storage device should be able to control these issues.

# Secure the network

The network is the first stop for traffic entering your environment from the Internet where everything must be treated as untrusted. The gateway or router that connects your company to the outside world is the closest thing left to a network perimeter. Thus, security must be layered and strong at this point.

Perhaps the most important weapon in your network security arsenal is a "next-generation" firewall (NGFW) such as the ones provided by Palo Alto Networks and Check Point. This is a hardware- or software-based network security system that is able to detect and block sophisticated attacks by enforcing security policies at the application level, as well as at the port and protocol level. Compared to older firewalls, an NGFW has more capabilities for traffic inspection to stop more types of threats.

Beyond a good firewall, additional security layers to consider adding include:

- **Intrusion Prevention System (IPS)** - An IPS is a control device that contains rules that determine if incoming traffic should be blocked because it is a known security problem.

- **Intrusion Detection System (IDS)** - An IDS is a visibility tool that allows a security professional to monitor traffic on the network to get a view of the security posture of the network.

By now you understand that building and maintaining a strong security platform is a complex task. What's more, it requires significant technical expertise that may be difficult to hire and retain. A good option for many SMBs is to outsource the monitoring and management of security devices and systems to a managed security service provider, or MSSP.
The common types of services provided by MSSPs include managed firewall, intrusion detection, virtual private network, vulnerability scanning and antiviral services.

An MSSP uses a high-availability security operation center (SOC) to provide 24x7 monitoring and alerting services. By outsourcing a portion of your necessary security services to an MSSP, you can reduce the number of operational security personnel you need to hire, train and retain to maintain an acceptable security posture.
Another option is to get advice from an experienced partner such as EY or IBM.

- **Anti-DDoS** - If you are concerned about distributed denial of service (DDoS attacks that cause service outages by overwhelming your devices, you might benefit from an anti-DDoS solution that looks for and drops traffic that is indicative of an attack. Talk to your ISP about their services and/or consider adding a cloud-based service or an on - premise appliance.

- **Geo-IP filtering** - A high percentage of attacks originate from countries like China, Indonesia, Taiwan, South Korea, Turkey and others where your company might have no legitimate business ties. A geo-IP filtering solution helps you weed out unwanted traffic from countries or regions where you don't do business. The bonus of this type of solution is that it makes all your other security devices more efficient because they will get far less traffic to process.

All of this together – at the endpoint and at the network level – builds you a strong moat and thick castle walls. These defenses are essential but you can't stop here. You have to assume that some flaming arrows will get over the castle walls, and this puts you in need of detection and response solutions.

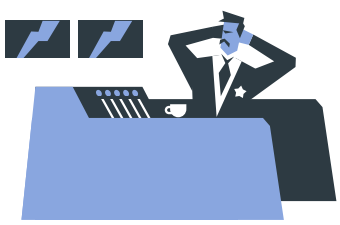
# Add Detection and Response Capabilities

Prevention is the best approach but it's not sufficient today. There's a saying among cyber security professionals: There are two kinds of organizations in this world—those whose computer systems have been compromised via a cyber attack, and those who just don't know yet that their systems have been compromised by an attack.

Security incident detection methods are expensive and complicated. They require the right combination of technology and highly skilled people. They typically depend on having data collection points throughout your network and then applying behavioral analysis on that near-real-time data to see if anything looks suspicious. This often requires looking for anomalous behavior and activity, such as someone trying to access a database that they have no business accessing.

A good detection system must correlate individual activities that, alone, might seem meaningless or harmless, but taken together indicate suspicious behavior worthy of a deeper look.
The technology to do this is very sophisticated, and even technology isn't enough. You need highly skilled people to investigate the alerts and make decisions about which alerts are important and require follow-up and which ones can be ignored. For most companies and especially SMBs, it's a real challenge to find and be able to afford people with the expertise to work in this environment.

**Because of the cost and complexity of operating a detection solution, SMBs are advised to consider outsourcing this function to a managed security service provider (MSSP). In this way you can feed your activity logs to the MSSP and they can monitor 24x7 and alert on truly important incidents that require your attention.**



Prevention and detection defenses are complementary and should be used together, not one or the other.

# Now Add Data Protection

What are attackers after? Primarily they want to gain access to information or data they can monetize (think ransomware) or use for an advantage; for example, credit card payment data, personally identifiable information (PII), private health information (PHI), intellectual property, and even your payroll and accounts payable systems.

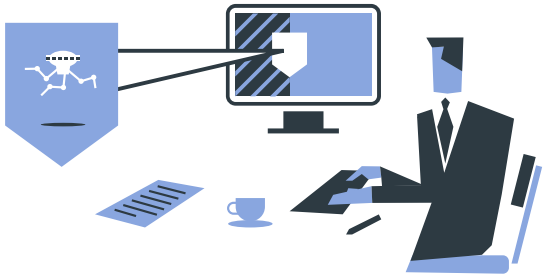
On the Dark Web, each record for payment card data can be worth a few dollars, and each record for PII or PHI can be worth much more than that to a cyber criminal. They have a high incentive to steal as much of this data as possible. And if they can get into your payroll or accounts payable systems, they can wire money outside your company in seconds. Even your intellectual property – your product blueprints, confidential marketing plans, customer lists, etc. – can fetch money from unscrupulous competitors looking for a competitive edge.

Even if you utilize the best preventative measures, and even if you faithfully monitor for indicators of compromise, your sensitive data and intellectual property still need an additional line of defense. This typically means encryption and/or tokenization. Encryption is a technology solution that puts sensitive data or textual information through a mathematical process called an algorithm to change the form of the data or information. The resultant value is called ciphertext. The original value of the information can be derived by using a key (a reverse algorithm) to "undo" the encryption process. Encryption can be used on numbers, alphanumeric strings, and even long passes of text.

Tokenization is a technology solution that replaces sensitive data with random data called a token as a substitute value. Instead of using an algorithm as encryption does, tokenization uses an index database called a token vault to hold the original data and an index to the substitute data. Tokenization is typically used for short alphanumeric data strings like credit card account numbers and social security numbers.

Either tokenization or encryption, or both, may be required by statute. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires merchants to protect payment card data through encryption and strongly recommends tokenization if the merchant wants to store data for use in other applications.

# And Don't Forget People!



Security technology is certainly essential but it can be all for naught if your workers aren't adequately trained to observe security-conscious work practices. People can help prevent attacks if they understand the ploys of social engineering used in phishing messages, or avoid using untrusted thumb drives, or carefully guard their login IDs and passwords.

**In the 2014 U.S. State of Cybercrime Survey by PwC, 42% of respondents said security education and awareness for new employees played a role in deterring potential attacks. The report also outlined a compelling financial case for security awareness training. Companies without security training for new hires reported annual financial losses of $683,000 for cyber security events, compared with companies with training that said average financial losses totaled $162,000.[9]**

While there's proven value in providing awareness training to new hires, all employees - including high level executives – should receive awareness training. All employees need to be empowered with the necessary knowledge to help prevent security incidents.

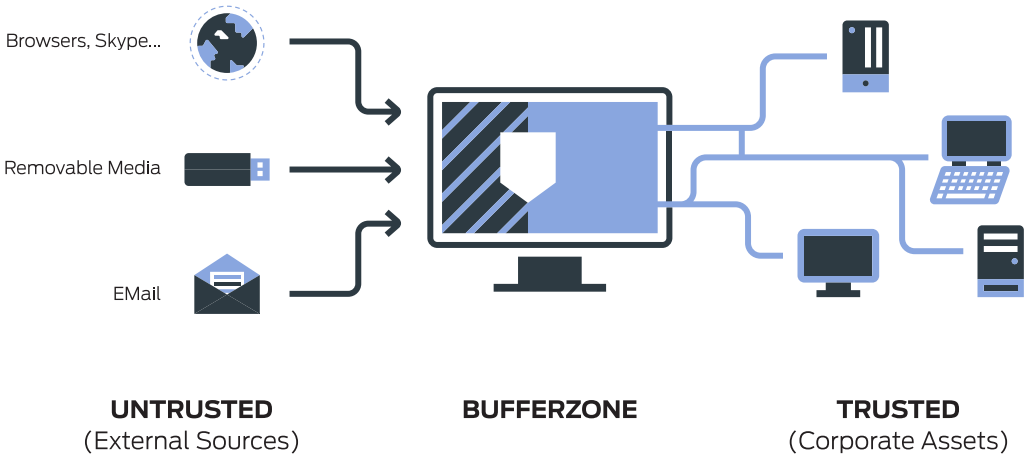
[9] PwC, 2014 U.S. State of Cybercrime Survey, June 2014

# BUFFERZONE Endpoint Security Stops Threats at Your Largest Attack Surface

We've outlined the general framework for building a layered security program for your computing environment. Now let's talk about protecting your largest and most vulnerable attack surface-the multitude of PCs spread throughout your organization.

BUFFERZONE endpoint security solutions protect your company from threats originating at endpoint PCs, including ransomware, zero-day exploits, drive-by downloads from the web, phishing and spear phishing scams, and advanced persistent threats (APTs). With cutting-edge containment, bridging and data intelligence, BUFFERZONE gives your employees seamless and secure access to their Internet applications, email and removable storage—thus preserving productivity while keeping the company safe.

BUFFERZONE's lightweight solution creates a container on the PC that isolates applications that come in contact with untrusted external sources such as browsers, email, removable media, web apps and more. The security is completely transparent so that from a user's perspective, the applications run normally, but from the security perspective, the applications are running in a separate, virtual container that provides complete segregation from the rest of the PC. This creates a buffer that prevents malware from escaping the container and infecting the endpoint and the company network beyond.

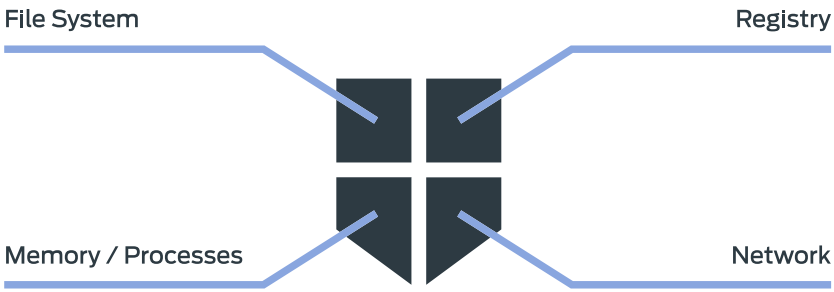



**BUFFERZONE creates an isolation container for untrusted data sources**

BUFFERZONE's containment technology isolates the entire PC application environment—memory as well as files, registry and more. Legitimate applications must have read/write access to files and registry data, but it is also through this file system and registry that viruses, worms, Trojan horses, spyware and other forms of malware are surreptitiously installed. BUFFERZONE solves this problem by allowing non- trusted applications to read from the file system and the registry, but as soon as they attempt to write or modify a file or registry key, the operations from this non-trusted application are redirected to the container. The end user is completely unaware of this security measure and is able to continue working with no disruption to normal productivity.

As a result, any harm inflicted by malware is completely sealed off in the virtual environment. Neither the endpoint nor the corporate network is infected through the strength of this separation process. New or previously unknown threats with unpredictable behaviors are contained just as effectively as known malware.

BUFFERZONE's endpoint security solution also includes a feature called Secure Bridge, a configurable process for extracting data from the container, removing any threats by disarming malicious code, and then moving the data into the trusted zone of the network. For example, when a worker opens an email attachment, that file is considered untrusted and placed in the isolation container. The attachment might be a legitimate document or spreadsheet the worker needs to perform his job. Once that file is rendered or proven to be harmless, the Secure Bridge moves it to the trusted environment where the worker can do what he needs with it.
The data intelligence collected from across all your endpoints can feed into security incident and event management (SIEM) and Big Data analytics to identify targeted attacks. The resulting information can be sent to your firewall and other security devices to improve their efficacy.
BUFFERZONE software is easily installed, updated and managed through common endpoint management platforms from companies like LANDesk, McAfee and Microsoft. It is transparent to the end users and can work on off-network devices. BUFFERZONE endpoint security solutions efficiently and effectively stop security incidents at your most vulnerable attack surface. They protect your computers without changing the way you work.



# Conclusion

All companies need to have a strong, layered information security program that protects in many dimensions. It's vital to prevent attacks in the first place, but you should also assume that some threats have found their way into your environment and you need to detect and respond to them.

**End users and their endpoint computers are your organization's biggest attack surface and largest point of vulnerability. The old strategy of simply running anti-virus software is no longer effective. But prevention is still more cost effective than after-the-fact detection, and cutting-edge containment solutions force endpoint attacks to die on the vine without spreading or causing harm. BUFFERZONE offers the leading endpoint threat containment solutions.**

**Detection and response should be complementary to prevention. Detection is expensive and complicated, and requires highly skilled people to follow up on alerts. SMBs are advised to consider a managed security service provider to help with detection capabilities. Moreover, once you move into the detection phase, you must recognize that damage may already be done and you are just trying to limit its scope. Data protection such as encryption and tokenization, as well as end user security awareness, round out the layers of a good information security framework.**
Are you ready to protect your company by stopping endpoint attacks cold before they can spread and raise havoc? Contact us to **begin a free trial of BUFFERZONE today**.