

Combating Today's Threats With **Multi-Layered Protection**

by Frank J. Ohlhorst

Introduction:

Businesses today are plagued by constantly evolving security risks. Online attacks are becoming more frequent, more sophisticated and more successful, creating a quandary for most businesses. How to combat these threats without impacting the budget and productivity adversely? That's the question most companies are trying to figure out. Add to that the compliance requirements for government data privacy regulations and the need to enforce acceptable use policies for email and the web, and it becomes readily apparent why most security solutions on the market today are not up to the mark. The fact is, there aren't many solutions that fit the bill.

As a workaround, many companies have resorted to combining multiple products from multiple vendors to stay one step ahead of the threats. However, that strategy has proven to be not only expensive but also complicated and prone to errors. What makes matters worse is that most businesses typically lack the time, budget, and IT resources to adequately defend themselves against all of today's sophisticated threats—and those that overcome the budgetary constraints face other problems, such as degraded system performance, caused by running multiple security technologies concurrently. Simply put, dealing with Trojans, botnets, spam, spyware, malware, malicious web sites, data loss, and data theft has become a chore that requires herculean efforts in terms of systems, software and staff.

Organizations of all sizes are looking for a better way to handle security. They're looking for a solution that is fast, simple and reliable, which leverages the latest security technologies and plugs all the holes. CA answers this demand with the Total Defense family, a product lineup designed to counter the latest threats and simplify the security process. Featuring innovations such centralized policy management console and pain-free installations, as well as new scanning technologies – CA can deliver on the promises of a secure system, which competitors have failed to accomplish.

Increasing Threats:

Malware has experienced an exponential growth and businesses have attempted to counter it by turning to more complicated, more invasive endpoint security products. These products have negatively affected user productivity by hobbling performance, consuming more clock cycles, delaying packets, and constantly notifying users of their security status with cryptic popup messages. Endpoints have suffered under the increasing demands of comprehensive security packages and users are starting to notice. Simple everyday operations such as opening files, launching applications and surfing the web are hindered by the processing overhead placed on system resources by security products. What's more, endpoint security products have become confusing and complicated, increasing end-user complaints while reducing productivity. That situation has led to many end-users removing or disabling their



**More Security. Less Cost.
Completely Installed.**

TOTAL DEFENSE™

MULTI-LAYERED INTERNET SECURITY

endpoint security products or simply ignoring the warnings offered, creating a security environment that is no longer sustainable.

Until recently, these problems, and many others like them, were accepted as the cost of doing business in a threat-rich environment. However, CA's Total Defense solutions are now countering these issues by offering innovative capabilities, such as an easy-to-understand client dashboard, high-performance scanning engine, intuitive messages and screens, as well as the ability to prevent end users from disabling protection. What's more remote deployment capabilities allow administrators to install CA's security silently on endpoints, as well as the ability to quickly remove old or unauthorized versions of security clients and replace those with the most current version of total defense - thanks to cloud deployment capabilities. Those features and many others stop the endpoint from being the weak link in the security chain, as long as those endpoints are protected by a member of CA's Total Defense solutions.

The Layered Approach:

Best practices dictate that security should be applied in layers, which helps to prevent threats from further infiltrating the network. The layered approach has proven to be effective in most security situations and threat environments. However, layers add latency, complexity and negatively impact the flow of data across the network. Today's security layers are far more complex than those used in the layered approach of the past - layers now not only apply to the threat classifications, but also to the location of the technology, such as on the endpoint, the server, the edge and the cloud. What's more, today's threat environment has further complicated security layering - to properly protect a network, technologies such as intrusion prevention, gateway security, content filtering, network access control, and spam filtering need to be integrated into the security layers, as well as the traditional anti-malware capabilities.

CA's Total Defense family of products takes an innovative approach towards layered security by offering an adaptable security infrastructure that places security technologies where they can be most effective. For example, content filtering can be handled at the gateway instead of on the desktop, while anti-spam capabilities can be integrated with the email server instead of being based in the cloud or forced into the desktop email client. With CA's security products, all of the components needed to enable maximum protection are included in the base install, allowing administrators to quickly add optional features to the security layer by just activating licenses. CA's modular style of security software deployment creates a layered security environment that can consist of as many layers as deemed necessary by the current threat environment. It also allows CA's security products to interact well with other security technologies, such as anti-spam appliances or hardware firewall deployed intrusion prevention technologies.

The Dangers of Complexity:

Although most security technologies are inherently complex, successful products hide that complexity from the end-user, while still enabling access to advanced capabilities and settings for network administrators. Reducing complexity is one of the key goals of CA's Total Defense product family.

Many security initiatives are derailed by overly complex installation schemes; CA's Total Defense products avoid that problem by offering a simplified installation paradigm, where initial installs can be performed remotely by CA support personnel, removing the burden of installation from harried administrators. Moreover, those installation routines are cloud based, eliminating the need to download installation files or obtain installation media.

What makes things even simpler is CA's unified security dashboard, which offers a centralized management point for administrators. The dashboard is laid out in a logical fashion with intuitive alerts that allow administrators to assess the security status of their network with just a glance.



More Security. Less Cost.
Completely Installed.

TOTAL DEFENSE™

MULTI-LAYERED INTERNET SECURITY

Complexity also impacts critical security areas such as policy creation and enforcement. Administrators have little desire to navigate through complex policy definitions and deployment schemes. Even worse is the fact that increased policy complexity often leads to improper policy creation, which results in critical elements being overlooked and not properly enforced. CA's Total Defense product family makes it easy to create, maintain and report on policies – thanks to a multitude of wizards, context-sensitive help and access to advanced technical support.

Evolving Threats = New tools

In the past year, malware has evolved in four major areas: bots, rogue security software, generic spyware, and targeted malware. Those threats have allowed criminals to find new ways to monetize unauthorized access, steal identities and gain access to proprietary intellectual property. Over the last year, malware has adapted better techniques for hiding and staying resident on new hosts, increasing the danger of identity theft and related fraud. Historically, security attacks get incrementally more dangerous over time and some attacks are bound to make major advancements if identified as successful. Malware will only get worse over the next year and grow beyond its current state of sophisticated botnets. Malicious code, too, is destined to become easier to use and criminals will gain access to full-management applications, improved toolkits and update mechanisms to carry out zero-day attacks and customizations. While that does not bode well for enterprise security pros, CA does offer the tools to secure systems with its Total Defense family of products.

CA has employed innovative techniques to combat those new threats and the enhanced threats that are sure to follow. By rethinking the online security environment, CA has developed new methods to combat malware and other threats, methods that do not rely on yesterday's technologies of signature files and manual product updates.

The Total Defense family leverages security methods like application white-listing, auto application identification, digital sandboxes, application monitoring, blended threat detection, and content filtering. Of course, security pros will need to perform due diligence for threat mitigation, and CA provides the tools that ease the process. The Total Defense family of products includes the ability to block IM traffic, P2P applications and access to known bad or suspicious websites. That protection can be enforced with easy-to-define policies that automatically define what a user can do. What's more, advanced reporting capabilities allow security pros to quickly and easily audit the security controls in place and identify any gaps in coverage due to improperly defined access policies. CA's multilayer approach to protection not only stops malware from entering the network, it prevents it from executing and also prevents unauthorized access into the network, combating malicious activity at all phases. Security scanning of email rounds out the protection.

Beyond Signatures:

Many security products rely on signatures to identify malware by comparing source files to a list of known bad identifiers. A few years ago, that methodology worked fine. However, the threats of today have increased significantly and signature file-based identification can only deal with known threats and is unable to deal with zero-day attacks or unknown threats, especially those that use a blended approach to compromise networks.

CA has developed new techniques to deal with malware, intrusions, spam, botnets and other attacks that do not rely on frequently updated signatures. First and foremost, a sophisticated policy distribution system controls how users interact with the internet, applications and communications technologies. By blocking access to suspicious information, most threats are neutralized effectively. Secondly, access to applications is controlled by a white-listing process,



More Security. Less Cost.
Completely Installed.

TOTAL DEFENSE™

MULTI-LAYERED INTERNET SECURITY

where known good applications have been vetted, known bad applications are blocked and new applications are thoroughly checked before allowing execution. Activities that are suspicious in nature are identified and blocked – a good example is online games, which can deliver malicious code. Another example is peer-to-peer file transfer services, which have been known to surreptitiously deliver embedded malware. Advanced content filtering technology rounds out the protection by preventing unauthorized content from traversing the network. CA's Total Defense family of products clearly goes beyond signature processing to combat today's threats and risks of tomorrow.

Location, Location, Location:

Protecting a PC from security threats is one of the top priorities for system administrators today. However, achieving an acceptable level of protection can be a difficult, if not an impossible task when using traditional security products. After all, PCs are expected to function reliably and securely, regardless of their physical locations.

Historically, on-premise PCs located behind the corporate firewall have always benefited from the highest levels of protection, but branch offices, home offices, mobile users and remote locations have been shortchanged when it comes to protection. Those PCs, and notebooks have often relied on locally installed, unmanaged consumer-grade anti-virus products to prevent attacks. Those consumer security solutions lack many of the features needed to effectively contain infections and mitigate risks. When any of those infected PCs are connected to the corporate network, there's a risk of the infection spreading and wrecking havoc, since malware can be transmitted from the remote PC onto the host network over a VPN or SSL connection and quickly spread to other PCs, servers or remote endpoints.

To combat newer threats, security pros need to deploy security products that not only protect PCs behind the

firewall, but also protect PCs out in the field. CA's Total Defense family offers that protection by using policy enforcement and push delivery of security technologies. CA's endpoint security client can be pushed down to a connected PC to perform scans and enforce policies, so infections cannot spread to the network through remote PCs. What's more, administrators can create policies that control the security on remote endpoints, even when they are not attached to the network.

Balancing Performance:

Complex security suites often come with an additional cost: slower PC performance. The performance impact associated with scanning files, opening applications, checking websites and filtering spam can be quite significant and can cause users to eschew some security functions in hopes of regaining performance. Security suites that don't leverage the latest technologies to improve performance can also impact performance across the network.

The potential for performance bottlenecks exists in several areas. Unified security products often place all of the scanning and filtering burden—sometimes with unnecessary and redundant scans—on the network gateway, which impacts all external communications. Add to that the performance overhead of policy enforcement, endpoint scanning and content filtering, and it becomes easy to see why poorly engineered security suites can adversely affect performance and productivity.

CA reduces the overhead of security and minimizes the impact on performance by using innovative technologies to maximize throughput. For example, white-listed applications are not scanned during execution, as long as they have been scanned originally and have not changed. Redundant scan protection eliminates unnecessary scans of static files, while scan caching stores previous scan results to speed up the overall security process. These technologies



More Security. Less Cost.
Completely Installed.

and others are combined with a multi-threaded, high-performance scanning engine, which maximizes performance while reducing operational overhead. CA's performance-enhancing technologies offer a noticeable improvement over previous-generation products. These innovative features also reduce bottlenecks in both network and desktop performance.

Why choose CA's Total Defense r12 products to protect your network?

The Total Defense r12 product family offers comprehensive network security solutions that are easy to use. The product line offers network administrators and security managers an action-based methodology to prevent, monitor and remediate almost any security threat. Network administrators and network security managers can stay on top of their security with up-to-date intelligent alerts and comprehensive reporting tools.

Available as an integrated suite and/or standalone solutions, Total Defense r12 offers five different levels of security to meet unique business needs. Administrators can start with any level and then upgrade to a more comprehensive solution.

Easy to scale and upgrade, Total Defense r12 offers flexibility and security that can adapt to the smallest of organizations and cover the largest corporations. It's built to handle today's changing cyberscape and prepared for tomorrow's online threats.

Total Defense r12 New & Improved Capabilities:

Total Defense r12 offers several industry-leading security technologies and introduces many new enhancements.

- ▶ **New:** Total Defense client with Integrated Anti-Malware and Host-Based Intrusion Prevention (functionality varies with presently installed product).
- ▶ **New:** Web-based management console that can be accessed securely from any connected, authorized, browser-equipped system.
- ▶ **New:** Network Access Protection capability enables users to conduct policy assessment, enforcement and non-compliance remediation.
- ▶ **New:** Enhanced reporting capabilities offer automatic and on-demand reports.
- ▶ **New:** Comprehensive Integrated Gateway Security Reporting (available with gateway security products) provides administrators with tangible evidence for validating security or remediating problems.
- ▶ **New:** Cloud-based licensing
- ▶ Remote Installation Services at no cost
- ▶ Automated endpoint discovery technology allows new and existing endpoints to be quickly protected by Total Defense client applications.
- ▶ A simplified deployment process allows the Total Defense client application to be automatically installed on newly detected endpoints.
- ▶ Endpoint protection architecture is designed to meet the needs of distributed organizations, scale appropriately and reduce the complexity associated with managing multiple endpoints.
- ▶ Role-based Access Control enables administrators to quickly define the appropriate levels of access for managing endpoints.
- ▶ Active Directory integration lets administrators enforce security policies across the enterprise.



More Security. Less Cost.
Completely Installed.