



F R O S T & S U L L I V A N

50 Years of Growth, Innovation and Leadership

Advanced Threat Landscape: What Organizations Need to Know

A Frost & Sullivan
White Paper

www.frost.com

Current Cyber Threats Impacting Organizations Today.....	3
<i>Corporate Email Systems</i>	<i>4</i>
<i>BYOD</i>	<i>4</i>
<i>Social Networks.....</i>	<i>4</i>
<i>Cybercriminals are Changing Attack Plans</i>	<i>4</i>
Misconceptions on Security Considered the Weakest Link.....	5
Is Endpoint Security Sufficient (Antivirus Solutions)?	6
<i>The Old Enemies.....</i>	<i>6</i>
<i>The New Enemies.....</i>	<i>6</i>
<i>A New Security Approach Needed.....</i>	<i>7</i>
Challenges in Protecting the Critical Infrastructure.....	8
<i>High-Value Targets:</i>	
<i>Domain Controllers are the Keys to the Kingdom for Cybercriminals.....</i>	<i>8</i>
<i>Vulnerabilities within the Domain Controller Server Infrastructure.....</i>	<i>10</i>
<i>Server Protection Challenges in Virtualized Environments</i>	<i>10</i>
<i>Server Protection in a BYOD Work Environment.....</i>	<i>11</i>
<i>Application Control</i>	<i>11</i>
<i>Lack of Standardization</i>	<i>12</i>
<i>Types of Data Cybercriminals Target.....</i>	<i>12</i>
Frost & Sullivan Recommends Trust-Based Server Security Solutions.....	13
Bit9’s Server Security: A Complete Enterprise Security	
Solution that Protects Against Advanced Threats	14
<i>Closing the Gap in Server Protection</i>	<i>14</i>
<i>File Integrity and Monitoring for Security Compliance</i>	<i>14</i>
<i>Email Systems, BYOD and Social Networks Covered.....</i>	<i>15</i>
Final Thoughts	15

CURRENT CYBER THREATS IMPACTING ORGANIZATIONS TODAY

With increased spending on IT resources since 2011, businesses expect rising customer demand for services such as online banking, cloud data storage, and social networking over the next three years. Organizations are responding to these business challenges by budgeting for additional capital expenditures on innovative IT strategies like big data analytics and virtualization technology. However, these new strategies call for more efficient IT security solutions that protect valuable assets, including mission-critical servers containing sensitive credentials that protect intellectual property (IP) data. This is because 2011 demonstrated how advanced threats were able to penetrate an organization's security architecture, resulting in a number of data breaches. Companies targeted by these advanced attacks included major companies like Sony¹ and RSA² Security and were considered the most significant security incidents recorded for the year. 2012 has also seen major security breaches involving companies such as LinkedIn, Yahoo, Zappos, eHarmony, and Global Payment Systems³. As a result, business leaders increased security spending to prevent further costly data loss incidents.⁴ Unfortunately, many organizations have chosen a security solution incapable of handling today's advanced threats.

Advanced threats are designed for the sole purpose of extracting data while avoiding detection in a stealthy, calculated manner. In 2011, 94 percent of data loss incidents were a direct result of server vulnerabilities.⁵ Most security intelligence analysts understand this, but there is a huge gap in understanding how to manage against advanced threats in today's IT environment. The origin of the problem can be traced to poor deciphering of what is considered malicious code or incomplete attack analysis on network anomalies. Furthermore, many IT administrators rely solely on antivirus or host intrusion prevention systems (HIPS) on their servers and endpoint devices, satisfied that these solutions are sufficient against advanced threats. Also, most organizations are unaware that an attack has already been initiated within their infrastructure due to the numerous business processes and changes taking place within their servers (system upgrades/expansion, change processes, security polices, etc.), along with the lack of qualified security resources available to detect, monitor, and mitigate these new advanced threats. Finally, signature-based and blacklisting techniques are simply not effective against the surge of new malware overwhelming IT administrators. This presents an unexpected dilemma to IT administrators because cybercriminals can set stealthy exfiltration points within the infrastructure, targeting servers with collateral information for data extraction. Consequently, unnecessary data breaches and irreparable damage to their company reputation can occur.

¹ <http://www.cnn.com/2011/TECH/gaming.gadgets/04/26/playstation.network.hack/index.html>

² http://www.msnbc.msn.com/id/42152645/ns/technology_and_science-security/t/rsa-security-firm-hit-sophisticated-hackers/

³ <http://abcnews.go.com/Technology/linkedin-hack-latest-blow-online-confidence/story?id=16513116>

⁴ <http://www.frost.com/p586>

⁵ http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Currently, advanced threats are using many attack vectors to steal IP data. A short list of attack channels that potentially pose the greatest threat to organizations' IT servers today are:

- Corporate Email Systems
- Bring Your Own Device (BYOD)
- Social Networks

Corporate Email Systems

Corporate email systems are prone to spear phishing attacks, which are usually tied to an Advanced Persistent Threat (APT). APTs will almost constantly use spear phishing techniques to deceive corporate users. Once the malicious payload has infected the user's client machine, the process begins and ultimately concludes with stolen IP data from servers. Spear phishing continues to be an effective social engineering tactic that poses the greatest risk to organizations.

BYOD

Businesses adopting the BYOD model for the sake of cutting expenses also bring considerable security risks into its IT infrastructure. Unmanaged devices pose unpredictable levels of risk to corporate IP data due to weak personal passwords and inefficient device management across the enterprise. And with mobile malware increasing at unprecedented levels on smartphones and tablets, IT servers are now becoming more susceptible to these advanced attacks. To be sure, malware authors will certainly take advantage of targeting these devices for IP data extraction.

Social Networks

Social networks are also a growing risk factor for most of the enterprises. Employees use social networking sites to promote and share product marketing announcements and for business-to-business (B2B) relationships. But with malware authors using social engineering tactics by posing as business contacts, users can be tricked by these fake profiles and will click on URL links that lead to malicious sites.

Cybercriminals are Changing Attack Plans

What organizations really need to understand is that cybercriminals are changing their attack plans. They are no longer pursuing Web, email, or storage servers directly. Instead, domain controllers are the primary servers targeted today. Domain controllers are servers that contain database directory stores, such as Microsoft's directory services (Active Directory), which are used for authentication and authorization for each user, group, and device. These servers are essentially master key vaults for the entire enterprise that allow users,

applications, and other servers to gain access to confidential assets. For cybercriminals, these servers can provide a strategic advantage: Once they are able to infiltrate and extract the enterprise credentials from the domain controllers, they are able to navigate the network freely while stealing IP data under the enterprise's radar. Even more concerning is the speed and methodology attackers implement in these advanced attacks allow them to bypass traditional detection systems for long periods of time.

Business leaders understand there are no silver bullets to resolve these attacks; however, they are asking two main questions:

1. When will these advanced attacks happen?
2. How will they respond?

In many cases, it's clear that most advanced attacks occur externally from perpetrators, including nation states, hacktivists, and cybercriminals. In other cases, however, the attack begins internally as a result of intentional or unintentional acts by disgruntled employees, executives, internal contractors, etc. More importantly, business leaders want security professionals to understand the methodology attackers use so they can improve their IT security posture. It seems clear that all businesses can expect to endure a persistent proliferation of external and internal advanced attacks targeting critical assets in the near future if it hasn't happened already.

MISCONCEPTIONS ON SECURITY CONSIDERED THE WEAKEST LINK

Most organizations are diligently trying to secure valuable data within their network environments. However, there is a false impression that strong security is overlaying their network infrastructure, leading to unacceptable risks for data loss. IT administrators are improperly focusing security efforts on hosted IPS or antivirus solutions on servers. While these solutions are important, they are not sufficient protection against advanced attacks on servers. This is because cybercriminals have developed attack strategies capable of circumventing these types of standalone security solutions.

The issue is the customer's perception that certain standalone network or endpoint security solutions provide higher levels of IP data protection than what currently exists. For example, if customers only deploy a data loss prevention (DLP) solution on mobile or laptop devices, they feel it will prevent data loss. Or if they rely solely on an antivirus or encryption solution, they perceive it should ensure confidentiality and integrity requirements across all endpoints.

“Advanced botnets compared to basic botnets have the ability to use cryptography and countermeasures, making it difficult to track and shut them down.”

IT administrators can implement user and access management to reduce IP data loss and boost security confidence, but that strategy substantially increases IT management costs when IT administrators are forced to manually check all user roles, especially in companies with large headcounts.

To prevent data breaches and negative publicity, security strategy needs to move forward to protect against today’s advanced threats.

IS ENDPOINT SECURITY SUFFICIENT (ANTIVIRUS SOLUTIONS)?

Endpoint security solutions have evolved fairly well when contrasted against IT advances. During the early stages of Windows, the Disk Operating System (DOS) was the primary target for hackers and was considered the endpoint for security solutions. Now, IT architectures have adapted to models such as cloud computing, mobile communication, and virtualization. Endpoints are still considered an important perimeter for all enterprises, but trusting each endpoint device that enters the network is difficult to manage in this new IT environment.

The Old Enemies

Standalone worms, Trojan horses, viruses, and botnet attacks were the top security challenges in the early millennium. These threats caused global damages exceeding \$60 billion USD between 2001-2003.⁶ Endpoint security vendors raced against time to identify a threat, create a patch, and distribute it to endpoint devices to quarantine each new threat. It also seemed that signature-based detection and blacklisting solutions were becoming the de facto security approach to defeat these threats. For a brief period it seemed that endpoint security vendors were developing a strategic advantage over the virus writers, but as time progressed, the threats evolved into a new form: malware.

The New Enemies

Malware is, quite simply, a set of malicious programs that includes Trojan horses, viruses, rootkits, worms, and other new threat variants. Examples include Flame, Duqu, Stuxnet, advanced botnets, and many others. Botnets, in particular, have advanced as well. Advanced botnets compared to basic botnets have the ability to use cryptography and countermeasures, making it difficult to track and shut them down. The main difference is that most malware is specifically designed to steal critical or sensitive data for monetary gain or economic advantage (nation state economic espionage⁷). Unlike standalone viruses and Trojan horses, malware payloads are designed to bypass traditional endpoint security solutions. Further, today’s malware evolves almost every 20 seconds into new and more

⁶ <http://www.infosecurity-magazine.com/view/15412/first-decade-of-the-century-a-boon-for-cybercrime-says-mcafee/>

⁷ <http://www.frost.com/q253015225>

⁸ http://www.sans.org/reading_room/whitepapers/threats/phishing-analysis-growing-problem_1417

dangerous variants; it can be deployed in a variety of forms and can use numerous attack strategies. Strategies include infected USB thumb drives left in places to tempt employees to pick up the device and insert into a client machine, unknowingly initiating an advanced attack. Spear phishing is another top attack strategy due to its success rate.⁸ Regardless of the attack strategy used, advanced threats are faster, more effective, and some can bring an enterprise network to a complete system halt in less than a minute.

A New Security Approach Needed

The evolution of advanced threats requires forward-thinking IT administrators to understand and acknowledge that it is impossible for endpoint security solutions that rely on blacklisting and antivirus technology to protect an organization against these serious new threats. By the time a new patch or signature is created and distributed to thousands of devices within the enterprise, 10 new malicious variants have been developed. Protecting business-critical data from advanced threats requires a defense-in-depth security strategy. Attack vectors are expanding at a rapid rate as IT systems increase in complexity and scalability. As these IT resources expand within enterprises, reliability and manageability can suffer while overseeing tens of thousands of endpoint devices within a typical medium-to-large enterprise.

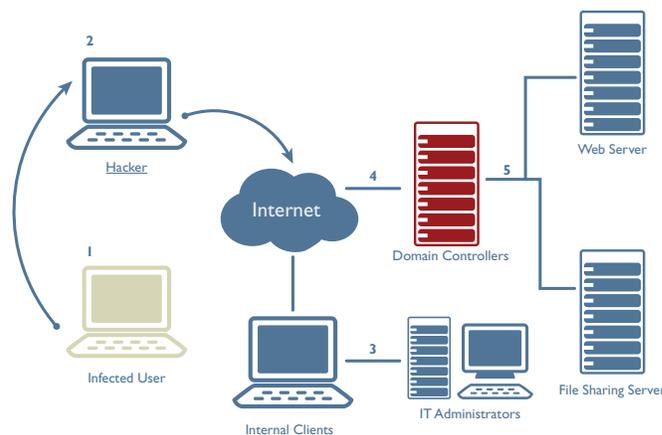
The sheer magnitude of tasks burdening IT administrators is one of many reasons why endpoint solutions are not enough to protect against advanced threats. Traditional antivirus technologies only address known malware codebases and signatures. When unknown software is introduced, it can present opportunistic threats, targeted threats, or both against the organization.

CHALLENGES IN PROTECTING THE CRITICAL INFRASTRUCTURE

High-Value Targets: Domain Controllers are the Keys to the Kingdom for Cybercriminals

Domain controllers are the keys to the enterprise kingdom, allowing users and applications to access confidential and sensitive data on servers. Cybercriminals in the past have targeted Web, file share, or email servers. However, they discovered that these were one-time attacks, as IT administrators would quickly detect attacks and patch the vulnerabilities. The cat-and-mouse game has changed since those days, and today's cybercriminals are actively seeking out longer-term attack strategies for larger and prolonged monetary gain. Figure 1.0 illustrates how cybercriminals target domain controllers while bypassing traditional security mechanisms.

Figure 1.0



Source: Frost & Sullivan analysis

1. First, the cybercriminal (hacker) will attack an employee's device using social engineering tactics (spear phishing emails, phone calls from attackers posing as help desk support). By using social attributes gathered from the Internet (LinkedIn, Facebook, etc.), cybercriminals attempt to convince a user to click on a malicious URL or execute an attachment with malware. These techniques either attempt to upload malware into the targeted client machine or trick the user into stating their username/password. Either way, the cybercriminal gains remote access privileges to the enterprise network. In most cases, cybercriminals will take advantage of vulnerability in Microsoft's NT LAN Manager (NTLM) framework using the username and password hashes to perform techniques like pass-the-hash. It is important to note that while Microsoft has advised organizations to use Kerberos, a much stronger security protocol, many other organizations today still use NTLM for legacy system support.
2. Once the cybercriminals have gained access, they begin scanning the network using free available tools on the Internet like Wireshark, Nmap, and Metasploit. The goal at this stage is to identify internal targets that are running applications or processes with domain controller credentials. Surprisingly, many enterprise networks allow internal

client machines (software developer, executives, contractors, etc.) with service accounts or applications running with domain controller credentials. These machines should not run these types of service accounts; domain controllers should only authenticate the user on these machines.

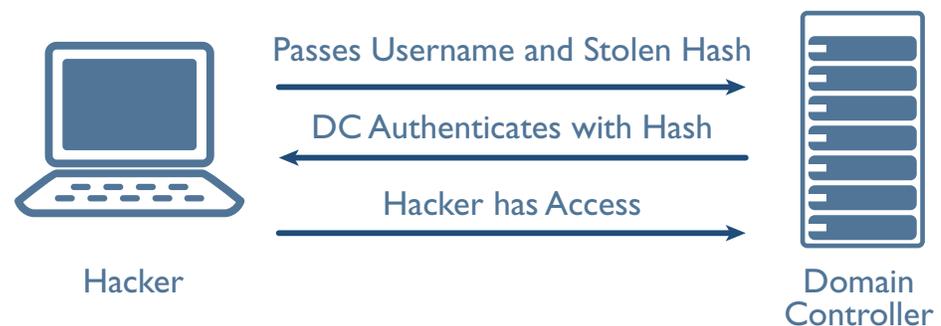
3. Next, the cybercriminals use the same strategies in step one (excluding the phone calls) on target machines to extract credentials (using password hashes again). At this point cybercriminals can gain access to the domain controllers and prepare their next step by uploading a malicious program into the domain controller server to read the entire database of credentials within the enterprise.
4. Once inside the domain controller, the cybercriminals will attempt to exfiltrate and decrypt all credentials. Although the credentials are encrypted, the use of hash decryption tools can make credentials readable. The tools needed for this step are widely available on the Internet as an offline executable or, in many cases, as an online database service (md5crack.com, Cain & Abel toolkits). Most concerning of all is how this stage of an attack allows cybercriminals to create new “dummy” accounts with administrative privileges.
5. After “dummy” accounts are created, cybercriminals are able to achieve their goal: to steal IP data from the Web, file, or database servers. Though this is the last critical step in the attack process, the hacker will not immediately begin the process; the main intent of this attack is to ensure stealth and persistence. The key strategy of this attack behavior is to bypass firewall alerts, HIPS, and other security systems in place, while critical IP data is stolen over a period of weeks, months, and sometimes years.

Typically, these attacks can take 15-20 minutes from the time of initiation to the last step of data extraction. However, it can take six months to a year before IT administrators detect IP data loss is occurring.

Vulnerabilities within the Domain Controller Server Infrastructure

There has been considerable improvement with Microsoft's domain controller's security architecture, but vulnerabilities remain for cybercriminals to take advantage of. Windows uses LAN Manager hashes (LM hashes) and/or Windows NT hashes (NT hashes) that are stored in Active Directory. These hashes are known to have a weak security design and prone to dictionary attacks and pass-the-hash attacks. Cybercriminals use tools to obtain hashes stored in a device's memory, which can contain administrative login hashes. Using a side channel attack technique, the cybercriminal can authenticate with a username and the stolen hash to gain access. Figure 1.2 illustrates this attack:

Figure 1.2



Source: Frost & Sullivan analysis

The cybercriminal is never required to crack the hash values. They simply “pass the hash” to the requested server (in this case, the DC server) to authenticate themselves.

As stated earlier, domain controllers run Active Directory. To date, Microsoft has recommended that enterprises use Kerberos and not NTLM since it does not support advanced encryption methods such as Advanced Encryption Standard (AES) and Secure Hash Algorithm 2 (SHA-2). However, because of legacy support and other IT requirements, many enterprises are still using NTLM for authentication. This presents a problem for many organizations with valuable IP data.

Server Protection Challenges in Virtualized Environments

Virtualized servers have offered organizations greater efficiency in terms of improved resource utilization, application isolation, and hardware independence. They allow for reduced costs in physical server deployment, cooling strategies, and other capital expenses. But this also increases the complexity level of management and monitoring services, diminishing visibility of security threats. Applications and data can reside on any computer node or database in a cluster of servers and storage devices. Understanding interdependencies within a virtualized server network has become more difficult. These issues have caused server protection concerns within virtualized environments.

In addition, virtualized servers also inherit virtual threats. Shared clipboard technology can allow malicious cybercriminals to transfer malware to different virtual machines (VM). Most VM servers allow keystroke logging that allows data to pass from virtual terminals to virtual machines. There is also the possibility of cybercriminals finding backdoors between guest and host machines. Rootkits could also insert themselves from the OS layer to the VM layer, causing the Rootkit to become invisible to traditional IPS systems before attacking physical machines through traditional attack vectors. Unlike physical servers, virtual servers cause greater complexity in the prevention of advanced attacks due to anti-VM techniques inside malware payloads.

Server Protection in a BYOD Work Environment

The introduction of mobile devices (smartphones and tablets) within enterprises has presented cost-saving benefits for businesses. However, these devices pose significant challenges for IT administrators responsible for securing IP data. First off, employees switch to BYOD models to gain freedom of choice, but most business users feel indifferent toward security measures already implemented in traditional network devices. An annoyance factor comes into play as users are introduced to security policies that control their Internet browser, logon authentication, and business applications that they must work with. Secondly, BYOD environments seem to boost user morale and productivity within the workplace.

Unfortunately, BYOD environments contain two major security challenges:

- Application Control
- Lack of Standardization

Application Control

One of the major concerns is gaining full visibility of mobile devices within an organization in terms of network and application control. The strategy used on PCs and laptops is not transferrable to mobile devices due to the nature of mobile architecture, where ubiquitous computing diminishes the entire enterprise security perimeter.

Mobile applications that access critical business data are either inefficiently monitored or not monitored at all due to weak solutions that don't encrypt data during transmission. Also, various mobile app stores (in the case of Android) exist that do not have strong vetting processes to validate apps and can introduce multiple vulnerabilities to the enterprise. Jail-broken Apple (iOS) devices, such as the iPad and iPhone, also pose significant threats to the network. This is because iOS users with jail-broken devices visit third-party app stores that allow them to download free versions of popular apps with questionable provenance. These application-control issues allow cybercriminals to place malware onto mobile devices before HIPS or endpoint solutions can detect and mitigate a security issue that can lead to a data breach. By using the same Command & Control (C&C) servers and malicious technology, cybercriminals are able to extract IP data from domain controllers, beginning at the mobile device-level.

Lack of Standardization

There are at least four mobile operating systems commonly used in organizations today: Blackberry OS, iOS, Windows Phone OS, and Android, with iOS and Android dominating enterprise BYOD environments. However, the standardization of mobile security is poor and the variety of mobile OS' hinders the implementation of firm security standards for mobile protection. High complexity in managing patches and updating multiple OS devices has contributed to making the challenge more difficult.

A good example of this challenge can be found with mobile encryption. The encryption standard used on traditional laptops/PCs is not entirely supported on most mobile devices. Android devices currently do not enable encryption by default. In fact, earlier versions of Android (before 3.0) did not have encryption capabilities and required users to download and install third-party encryption tools. Aside from the Android OS, MDM tools must stay current with numerous security updates in all mobile OS'. Without standardization, the potential remains for different browser exploits between mobile OS environments, along with meager security practices such as implementing weak security PIN numbers, peer-to-peer (P2P) transfers, and stolen devices. In the case of stolen devices, for example, remote data wiping could be missing from a particular mobile OS.

Types of Data Cybercriminals Target

Cybercriminals are targeting data from servers they believe to be valuable. These data types include:

Figure 2:



Source: Frost & Sullivan analysis

Banking and credit card information are the most targeted data types by cybercriminals.⁹ Because of the large number of customers in major banks, cybercriminals get their highest return on investment (ROI) targeting bank employees. The second most targeted data type after banking/credit card information is personal data. This information is more valuable than most employers think since it can be used by organized crime, botnet controllers, and identity thieves to generate illicit profits in the hundreds of millions. Government agencies, technology companies, and public utilities are also at high risk of advanced cyber-attacks.

⁹ http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Trade secrets, strategic planning and economic disruption are primary motives behind these attacks. The manner in which these attacks are carried out is similar to domain controller attacks, with the exception of the energy and public utility sectors that rely on enclave systems consisting of hardened UNIX servers, mainframes, and other open-end systems. UNIX systems running Samba as an integrated suite to communicate with domain controllers are vulnerable, where cybercriminals can gain root access if Samba is configured improperly.

What is important to note, is most of this data can be correlated and used for sophisticated social engineering attacks. The process of developing personal profiles from the Internet by way of data correlation can lead to successful spear phishing attack campaigns toward high-profile executives and other employees tied to valuable assets. Ultimately, credit card information, trade secrets, and banking information residing on Web and other data repository servers are the main targets.

FROST & SULLIVAN RECOMMENDS TRUST-BASED SECURITY SOLUTIONS

Signature-based, standalone blacklisting, HIPS, and other endpoint solutions are simply not capable of coping with advanced threats impacting companies today. With new malware families and variants being created in the tens of millions each year, endpoint security is unable to detect and mitigate malware threats successfully. In addition, firewall solutions are considered ineffective because of known ports and services commonly exploited by cybercriminals. In the end however, users are still the weakest link; it only takes a single click on a malicious URL within a browser for malware to bypass firewall policies. Managing today's security challenges can lead to substantially higher IT management costs and still fail to adequately address new advanced threats. That is why Frost & Sullivan believes that security best practices should include the adoption of trust-based security solutions.

Trust-based security technologies allow permitted, known applications and services to execute and run within the organization's infrastructure. This is accomplished by using a trusted file list of known heterogeneous applications that are hashed. Using a strong hashed list strategy can offer the strongest security control system over an organization's executable files that access IP data. In a trust-based security environment, cybercriminals attempting to drop malicious payloads in remote, internal, and domain controller machines will face new security safeguards. This advanced whitelisting approach checks against a known list of applications to see if the application from the cybercriminal is legitimate and permitted for installation. This process prevents any unauthorized, malicious application from infiltrating the network and exfiltrating critical business data.

Trust-based security technologies increase operational efficiency while reducing IT management costs and overall security risk. Taking ROI into consideration, application control dramatically decreases IT costs by automating IT security tasks and reducing the need to perform data recovery tasks following destructive breach of security.

BIT9 SERVER SECURITY: A COMPLETE ENTERPRISE SECURITY SOLUTION THAT PROTECTS AGAINST ADVANCED THREATS

Bit9 has responded to the advanced threat dilemma for all industries by providing companies with an advanced strategic security methodology using four key elements: Trust, Detect, Protect and Measure. Not only does Bit9 believe its approach is the right one, so do customers. It was shown that Bit9 was the only security company to stop Flame malware, a claim as yet undisputed by other security vendors.

Closing the Gap in Server Protection

Bit9's Server Security solution addresses the issues that companies face with corporate email systems, BYOD environments, and social network threats that occur between endpoints and servers. This solution relies on a trust-based security platform that gives customers the ability to:

- Create policies for trusted software and prevent anything else from running
- Detect, in real time, authorized and unauthorized changes that may represent a server attack
- Protect corporate IP from the advanced threat by blocking untrusted software
- Continuously measure their security posture to see if they have drifted from their gold image
- Achieve optimal virtual system performance and protection
- Monitor memory and registry to prevent buffer overflow injections, or changes to registry keys with custom registry protection

File Integrity and Monitoring for Security Compliance

An important feature of note offered by the Bit9 Server Security solution is the ability to ensure integrity of configuration files. This feature allows you to monitor, control, and prevent unauthorized activities such as permission changes and other changes that signify an advanced attack. It also provides critical log files that could prompt IT administrators to take mitigation action during an advanced attack.

With these features, the Bit9 Server Security solution provides information assurance and integrity between endpoints and servers. Domain controllers will have unyielding protection against malicious attacks attempting to embed into servers. Just as important, IT administrators will gain the upper hand in the advanced threat battle by lowering IT management costs up to 40% and achieving higher performance when running a trust-based security solution.

Email Systems, BYOD, and Social Networks Covered

Using Bit9's trust-based model, endpoint devices can also be secured. In the case of remote devices and BYOD environments, baseline images are used that will only allow trusted services and applications to install and execute on these devices. This eliminates the IT administrators' burden of patching updates with inefficient antivirus solutions. Bit9 can cover most endpoint devices including laptops, desktops, SCADA terminals and Point-of-Sale (POS) terminals running Windows environments. Bit9's solution can prevent malicious URL's in email and social networks from successfully completing an attack.

Bit9 recommends a top-down security approach that is deployed in four phases:

1. Protect your critical infrastructure first by locking down domain controllers.
2. Next, expand the security ring to protect critical application/file servers that carry targeted IP data.
3. Lock down internal assets such as workstations, laptops running inside the network.
4. Lastly, expand your security coverage to remote workers.

FINAL THOUGHTS

Cybercriminals are carefully crafting malicious payloads against targeted users and devices for the highest monetary gain and it is clear that organizations cannot continue to rely solely on endpoint security; a defense-in-depth strategy is needed. Advanced threats continue to increase in complexity and numbers and there is no question that they will continue to regularly bypass traditional security firewalls, HIPS and antivirus solutions. It is clear to cybercriminals that domain controllers are the most valuable primary targets and remote users are the gateways to these assets.

Bit9 has shown thought leadership in its response to the advanced threat challenge and has proved the efficacy of its Server Security solution against state sponsored malware. Using proactive, trust-based security technologies, organizations are assured real time detection and protection of their business critical data. In addition, IT administrators are given the ease of application control and a low cost process. The era of laborious application whitelisting tasks has been eliminated with Bit9. Organizations that are serious about data protection must acknowledge that traditional security measures cannot effectively counter advanced threats and should evaluate Bit9 to address today's advanced threat challenges.

Silicon Valley

331 E. Evelyn Ave. Suite 100
 Mountain View, CA 94041
 Tel 650.475.4500
 Fax 650.475.1570

San Antonio

7550 West Interstate 10, Suite 400,
 San Antonio, Texas 78229-5616
 Tel 210.348.1000
 Fax 210.348.1003

London

4, Grosvenor Gardens,
 London SW1W 0DH, UK
 Tel 44(0)20 7730 3438
 Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:

Frost & Sullivan
 331 E. Evelyn Ave. Suite 100
 Mountain View, CA 94041

Auckland

Bahrain

Bangkok

Beijing

Bengaluru

Bogotá

Buenos Aires

Cape Town

Chennai

Colombo

Delhi / NCR

Dhaka

Dubai

Frankfurt

Hong Kong

Istanbul

Jakarta

Kolkata

Kuala Lumpur

London

Manhattan

Mexico City

Miami

Milan

Mumbai

Moscow

Oxford

Paris

Pune

Rockville Centre

San Antonio

São Paulo

Seoul

Shanghai

Shenzhen

Silicon Valley

Singapore

Sophia Antipolis

Sydney

Taipei

Tel Aviv

Tokyo

Toronto

Warsaw

Washington, DC