Best Practices for Securing Remote and Mobile Devices
# Table of Contents

- **Executive Summary** .................................................. 3
- **The Rise of Mobile and Remote Computing** .................. 3
  - Risks from Remote Computing .................................. 3
  - Risks for Mobile Workers ........................................ 3
  - And the Risks are Growing ....................................... 4
- **Host-Based Application and System Firewalls** ............. 4
- **Intrusion Prevention** ............................................... 4
- **Anti-Spyware** ....................................................... 5
- **Anti-Phishing** ..................................................... 5
- **Vulnerability Management** .................................... 5
- **Piecemeal Solutions are Ineffective** ......................... 6
- **Best Practices Security Solution for Mobile and Remote Computing** .......... 6
  - **Host-based Security for Mobile and Remote Machines** ... 7
  - **Application and System firewalls that limit the attack surface** 7
  - **Intrusion prevention to protect unpatched machines against known attacks** 7
  - as well as zero-day attack ........................................ 7
  - **Protection from ID theft and spyware** ...................... 7
  - **Vulnerability auditing to ensure that remote and mobile machines contain** 7
    the latest patches and comply with corporate security policies .......... 7
  - **Secure access control to the corporate network over the VPN** .... 8
- **The BeyondTrust Solution** ....................................... 8
  - **Retina Endpoint Intrusion Prevention** ...................... 8
  - **Retina Scan on Connect** ...................................... 9
- **The BeyondTrust Solution** ....................................... 9
  - **Retina Endpoint Intrusion Prevention** ...................... 9
- **Additional Benefits** ............................................. 10
- **About BeyondTrust** ............................................... 10
A best practices approach to mobile and remote security requires an integrated, comprehensive solution.

Executive Summary

As the number of mobile and remote workers has exploded over the past few years, so too have the security risks they pose. With the rise in new and blended threats that use multiple vectors of attack, these workers are increasingly vulnerable. They also pose a growing threat to the corporate network when hackers use vulnerabilities on these machines as conduits to the corporate network once these workers re-connect. Over the years, numerous technologies have been developed to address these security issues. But as the number, complexity, and severity of threats has grown, these point solutions are no longer adequate. Today, industry experts agree that the best method for securing mobile and remote machines, and the corporate networks they access via a virtual private network (VPN) or within the perimeter firewall, is an integrated, multi-level approach. This white paper describe best practices for securing mobile and remote machines and how BeyondTrust’s Retina® Endpoint Intrusion Prevention and Retina® Scan on Connect Solutions enable organizations to secure mobile and remote machines—and the broader corporate network—from today’s most sophisticated and blended threats.

The Rise of Mobile and Remote Computing

Over the past few years, the number of remote and mobile workers has grown dramatically. Forrester Research reports that roughly 82 percent of large companies now have VPNs in place, up sharply from 55 percent in 2003. InStat/MDR predicts that the number of mobile workers in the U.S. will reach 103 million by 2008, while by 2009 the number of mobile workers worldwide will reach 878 million. By the year 2010, the Gartner Group predicts that 80 percent of key business processes will involve the exchange of real-time information involving mobile workers. Yet at the same time, remote and mobile machines are posing greater risks.

RISKS FROM REMOTE COMPUTING

Organizations often assume that remote users are secure because they access the corporate network through a virtual private network (VPN). Yet while VPNs provide a tunneled connection that allows only authenticated users to access the corporate Intranet, they are not a complete, end-to-end solution. VPNs do not ensure that remote and mobile devices are free from software and configuration vulnerabilities, which could be used to propagate viruses or worms. These examples of malware are easily introduced via standard DSL or cable connections and as a result, remote machines can expose critical network assets to these vulnerabilities.

RISKS FOR MOBILE WORKERS

Likewise, mobile employees take their laptops home and on the road, then work from their new location in much the same way they would in the office—however now, they are without the protection of the corporate firewall. This leaves their systems exposed to viruses, worms, and other types of malware, increasing the risk that these machines will later be used by attackers to access the network illegally.

These machines eventually return to the corporate network, literally walking past the network firewall and are allowed to connect as trusted devices. If infected, a machine can easily become a conduit for introducing malicious code into the corporate environment.
AND THE RISKS ARE GROWING

Even as the number of mobile and remote users increases so too does their risks. Today, the number of attacks and their complexity are growing, along with their associated risks. While in the past, there were only a few primary types of well understood attacks, it is now impossible to keep up with the number of threats organizations face today. In the late ‘90s, attacks were typically launched by hackers simply to see if they could be done, or by people motivated to perform a digital prank or to make a statement. Attackers today are far more likely to be motivated by the opportunity to steal data. This can be seen in increases in phishing attacks that socially engineer unsuspecting users into divulging personal information, such as credit card numbers or social security numbers that can be used for identity theft. Indeed, a recent survey of 5,000 adult Internet users conducted by the Gartner Group found that the number of people targeted by phishing email attacks grew 28 percent in the year ending May 2005. Attackers are also increasingly targeting mobile and remote machines. For example, blended threats (which exploit several different flaws simultaneously, such as sending a virus via an e-mail attachment along with a Trojan horse embedded in an HTML file) are specifically targeting laptops outside the firewall to gain unauthorized access to the corporate network during an ISP connection.

HOST-BASED APPLICATION AND SYSTEM FIREWALLS

Traditionally, organizations have relied on anti-virus software and personal firewalls residing on the individual machine to secure remote and mobile devices from attack. Using such host-based application and system firewalls, the organization can specify which ports systems will leave open and which applications are allowed to communicate with which other machines and applications. These solutions reduce the organization’s “attack surface,” meaning the amount of software that can be exposed and thus vulnerable to attack. For example, you can use a firewall to filter SQL Database traffic for all servers except the Web Server performing SQL transactions and the SQL Server itself. In this way, fewer systems are open to attempted exploits of SQL Server bugs. However, firewalls do not examine the traffic that permitted applications send to determine whether it is malicious. Thus, attackers are able to exploit software vulnerabilities in permitted applications. For example, viruses, worms, and Trojans are commonly distributed using protocols that are inherently trusted, such as e-mail and Web traffic, and are therefore allowed by firewalls. For the same reason, firewalls cannot guard against blended threats. To mitigate these vulnerabilities using a firewall, you would need to firewall the affected ports, which is impractical because they are commonly used for everything from file sharing to patch management to authentication and this would preclude these functions from operating properly. What are the available options? Shut down the firewall and lose security protection, create extensive workarounds, or combine host-based firewalls with additional protection.

INTRUSION PREVENTION

Overcoming the limitations of firewalls requires a second line of defense—intrusion prevention solutions use an intelligent analysis of Internet traffic to detect that telltale patterns that identify malicious code. Some intrusion prevention devices compare network traffic patterns against a database of known attack signatures to guard against previously documented types of attacks. As threats continue to grow more quickly than the ability to respond, intrusion prevention solutions have begun to provide more proactive means of identifying and protecting against emerging attacks through behavior-based profiling techniques that observe deviations from expected system behavior.
However, behavior profiles can be problematic for IT departments. Some require administrators to teach the solutions about how attacks operate in time-consuming detail. Others come with a default set of application profiles. However, most systems are not identical to what is found in these pre-packaged profiles—while many environments employ third-party software that may not be profiled. Thus, regardless of the profiling techniques used, intrusion prevention profiles are often incomplete. Another drawback of behavior-profiling technologies is that they often result in large numbers of false positives. Because they must examine all network traffic, they can become a bottleneck. Additionally, these solutions are unable to prevent attacks before some malicious code has begun to execute on the system; the only way to stop this code is to terminate its execution by terminating the thread within the application, the entire application, or by rebooting the entire workstation. Thus, while intrusion prevention is a good last defense, it is best used in combination with other forms of protection.

**ANTI-SPYWARE**

A number of anti-spyware solutions have sprung up to address this growing threat. These solutions detect spyware programs, tell users where they're located, give them a risk rating, and recommend what action to take. Users can then either disable the program or permanently remove it.

**ANTI-PHISHING**

Phishing attempts, orchestrated by organized criminals, use social engineering techniques to trick end users into revealing personal information, such as social security numbers, and are a major factor in identity theft. Anti-phishing solutions monitor the Web sites users visit in real time and alert users to sites that may be potentially bogus based on techniques such as blacklists of known fraudulent websites, white lists of good sites and analyses of web addresses and web pages.

**VULNERABILITY MANAGEMENT**

CERT reports that more than 95 percent of all network security issues involve the exploitation of known vulnerabilities that can be avoided through the timely application of patches and by following security policies. Yet, despite the fact that the window of time between the discovery of a vulnerability and its exploitation by hackers is shrinking, making it essential to apply patches quickly, “security drift” is a tremendous problem with mobile and remote users. It is easy for end users to decline anti-virus updates. And since users are out of the office, it is difficult for IT to ensure that these machines are updated with the latest security patches. Indeed, according to a study by Quality Resource Associates, 89% of IT desktop managers surveyed said that remote and mobile endpoints make it more difficult to comply with IT, financial, regulatory, or security policies. When asked what would make their job easier, most desktop managers (64%) wanted the ability to verify in real time that all remote and mobile endpoints are in IT and regulatory compliance.
For IT to be confident mobile and remote machines are secure against latest known threats requires a solution which guarantees that the necessary fixes or patches are in place and the machines are in compliance with latest corporate policies; for example, requiring that machines contain the latest antivirus software. Two types of tools are available to assess vulnerabilities on mobile and remote devices. Network-based assessment tools, which reside on VPN gateways and detect open ports, identify services running on these ports, and reveal possible vulnerabilities associated with these services. These solutions can screen mobile devices before they connect to the corporate network, and deny non compliant machines access. Host-based vulnerability assessment tools reside on the mobile or remote machine and audit the machine for system-level vulnerabilities including incorrect file permissions, registry permissions, and software configuration errors. They also ensure that the system is compliant with predefined company security policies. Some solutions advise administrators of necessary patches and software updates, others can even automatically correct the problems. However, these are standalone solutions that do not integrate with other security measures.

**PIECEMEAL SOLUTIONS ARE INEFFECTIVE**

While each of these individual solutions is worthwhile to address a particular aspect of end point security, none by itself is complete. Thus, none of these solutions can fully address today’s increasingly sophisticated threats.

**ANTI-PHISHING**

Phishing attempts, orchestrated by organized criminals, use social engineering techniques to trick end users into revealing personal information, such as social security numbers, and are a major factor in identity theft. Anti-phishing solutions monitor the Web sites users visit in real time and alert users to sites that may be potentially bogus based on techniques such as blacklists of known fraudulent websites, white lists of good sites and analyses of web addresses and web pages.

**Best Practices Security Solution for Mobile and Remote Computing**

Today, it is commonly understood that organizations should pursue a multi-layered approach to security management for mobile and remote workers that incorporates a complete range of functions; including existing anti-virus software, host-based application and system firewalls, proactive intrusion prevention, anti-spyware, anti-phishing, and vulnerability management. Such a comprehensive, well integrated approach makes it easier to address the exploding numbers of new vulnerabilities and the complex, blended threats attempting to leverage those vulnerabilities. Integrated solutions also reduce up-front costs—since they require purchasing and installing one, rather than multiple systems.

And they are easier to administer and maintain on an ongoing basis, for lower long-term total cost of ownership. Such an integrated solution should work in conjunction with existing anti-virus software and should incorporate the following components:
HOST-BASED SECURITY FOR MOBILE AND REMOTE MACHINES

Because mobile and remote machines operate outside the corporate firewall, these machines require individual, host-based protection that guards against a full range of known and unknown attacks as well as ensure these machines comply with security policies and latest patch levels.

APPLICATION AND SYSTEM FIREWALLS THAT LIMIT THE ATTACK SURFACE

While application and system firewalls are not the complete solution, they do reduce the possible attack surface by controlling which applications can communicate with which machines and which applications over which port and remain an integral part of a complete solution.

INTRUSION PREVENTION TO PROTECT UNPATCHED MACHINES AGAINST KNOWN ATTACKS AS WELL AS ZERO-DAY ATTACK

A best practices solution must integrate intrusion prevention technology that can examine network traffic flowing between permitted applications to ensure this traffic is legitimate. Intrusion prevention solutions should compare traffic against a database of known attacks. This database needs to be updated continuously to reflect constant research into new and emerging threats. It should also include sophisticated behavioral modeling to proactively guard against unknown, zero-day attacks, as well as provide a way for organizations to guard against known attacks while they test and apply patches. This allows organizations to patch during normally scheduled maintenance windows, rather than in a frantic response to a worm or virus outbreak.

PROTECTION FROM ID THEFT AND SPYWARE

A best-practices solution needs to actively block malware instances from being loaded into memory and give the option to quarantine or remove the suspected code, as well as the ability to scan the disk for existing spyware instances. It also needs to detect and classify phishing attempts made via various protocols, including the images used to convey these phishing attacks and warn users of possible attacks.

VULNERABILITY AUDITING TO ENSURE THAT REMOTE AND MOBILE MACHINES CONTAIN THE LATEST PATCHES AND COMPLY WITH CORPORATE SECURITY POLICIES

A best-practices, host-based vulnerability scanner will also scan the host machine on an ongoing basis and compare its configuration with a current database of known vulnerabilities. This vulnerability database must be updated with the latest information on emerging threats on an ongoing basis. The scanning solution should also make sure systems are in compliance with internal corporate security policies and configuration requirements, including the latest patch levels. Such vulnerability assessment will help organizations guard against known threats so they can focus on the more important dangers. It will also help prove the organization has done “due diligence” in performing basic system patches and fixing the well-known problems in case a security breach causes financial, legal, or regulatory problems.
SECURE ACCESS CONTROL TO THE CORPORATE NETWORK OVER THE VPN

Although corporate policy may require that remote and mobile machines be assessed for vulnerabilities, non-compliant machines may nonetheless attempt to access the corporate network. Therefore, organizations need to be able to validate host security by scanning devices during the login process before they connect over the VPN. This ensures that mobile and remote machines are free from vulnerabilities and in compliance with corporate security policies. Because corporations need to balance the need for user productivity with security requirements, they need to be able to create policies around access. Rather than banning all non-compliant machines outright, the scanning solution should be able to assess the risks devices pose to the network and communicate this information back to the VPN gateway so it can determine, based on company defined security policies, whether to grant a device full or partial access or to deny access altogether. These solutions might, for example, allow devices that do not fully comply with the latest security policies to still access the network, but limit access to certain applications and network resources, such as web-based email.

The BeyondTrust Solution

BeyondTrust is unique in offering a complete solution that addresses all of these best practices requirements with our Retina Endpoint Intrusion Prevention system and our Retina Scan on Connect solution for secure network access.

RETINA ENDPOINT INTRUSION PREVENTION

The Retina Endpoint Intrusion Prevention system integrates multiple layers of proven security technologies to proactively shield mobile and remote machines from known and unknown vulnerabilities. Retina combines and extends the technologies of intrusion prevention, personal firewalls, anti-spyware, identity theft protection/anti-phishing, application protection and BeyondTrust’s Retina vulnerability assessment scanner. These integrated protection layers work together to provide powerful protection of individual digital assets against targeted and mass propagated attacks. Through these capabilities, mobile and remote users, as well as the corporations to which they belong, benefit from:

- Protection from known and undefined vulnerabilities. The included Retina vulnerability assessment scanner continuously scans hosts for known vulnerabilities while Retina’s innovative approach to protocol analysis guards against zero day attacks.

- The ability to patch during normally scheduled maintenance windows, rather than in a frantic response to a worm or virus outbreak.

- The enforcement of policy compliance. Retina constantly audits systems for compliance with corporate security standard configurations thus reducing the risk associated with non-standard applications, such as outdated anti-virus deployments.

- Security for unsupported platforms. As vendors end support for legacy platforms, organizations are left with little recourse to protect assets running critical applications. Retina’s innovative IPS technology protects these systems without requiring a reduction in functionality.
RETINA SCAN ON CONNECT

Retina Scan on Connect ensures that devices connecting to the network through the VPN are free from threats and in compliance with IT security policies before they are allowed on the network. During the logon process, Retina Scan on Connect checks devices for vulnerabilities and minimum assurance levels, corporate security policy settings, misconfiguration, required patch levels, and other security settings. Based on its findings, Retina Scan on Connect provides the VPN gateway with a risk analysis of each device. This enables the gateway to determine, based on company-defined security policies, whether to grant a device full or partial access, or deny access altogether. Using Scan Connect, organizations benefit from the ability to:

- Quickly and accurately identify vulnerabilities on devices through non-intrusive scans that leverage Retina's vulnerability database—the most comprehensive CVE-compliant security database. BeyondTrust’s world renowned Research Team constantly updates this database.

- Create and implement custom corporate policy-driven scans to audit devices for compliance with internal security policy guidelines and configuration requirements, including the latest patch levels. Organizations can create custom audits and configure custom scans to assist with meeting any regulatory compliance requirements (SOX, HIPPA, GLB, etc) organizations may face.

The BeyondTrust Solution

BeyondTrust is unique in offering a complete solution that addresses all of these best practices requirements with our Retina Endpoint Intrusion Prevention system and our Retina Scan on Connect solution for secure network access.

RETINA ENDPOINT INTRUSION PREVENTION

The Retina Endpoint Intrusion Prevention system integrates multiple layers of proven security technologies to proactively shield mobile and remote machines from known and unknown vulnerabilities. Retina combines and extends the technologies of intrusion prevention, personal firewalls, anti-spyware, identity theft protection/anti-phishing, application protection and BeyondTrust’s Retina vulnerability assessment scanner. These integrated protection layers work together to provide powerful protection of individual digital assets against targeted and mass propagated attacks. Through these capabilities, mobile and remote users, as well as the corporations to which they belong, benefit from:

- Protection from known and undefined vulnerabilities. The included Retina vulnerability assessment scanner continuously scans hosts for known vulnerabilities while Retina's innovative approach to protocol analysis guards against zero day attacks.

- The ability to patch during normally scheduled maintenance windows, rather than in a frantic response to a worm or virus outbreak.

- The enforcement of policy compliance. Retina constantly audits systems for compliance with corporate security standard configurations thus reducing the risk associated with non-standard applications, such as outdated anti-virus deployments.

- Security for unsupported platforms. As vendors end support for legacy platforms, organizations are left with little recourse to protect assets running critical applications. Retina’s innovative IPS technology protects these systems without requiring a reduction in functionality.
Additional Benefits

Centralized Management

Large organizations can take advantage of BeyondTrust’s REM Security Management Console to manage security for their entire distributed network, including mobile and remote devices protected by Retina and VPN gateways protected by Retina Scan on Connect. Leveraging vulnerability, attack and policy related information provided by Retina and Retina in local or distributed environments, REM provides metrics and graphical representations of enterprise security risk. This allows administrators to quickly determine security status on several different levels – business unit, geographic location, operating system, etc. These risk views are completely customizable by the end user, so calculations can be made according to corporate policies, internal objectives, etc.

Conclusion

A best practices approach to mobile and remote security requires an integrated, comprehensive solution that addresses a wide range of sophisticated and blended, known and emerging security threats. With its Retina and Scan on Connect solutions, BeyondTrust offers such a best-practices approach. Retina incorporates local vulnerability assessment and threat protection that includes a host-based firewall, intrusion prevention, anti-spyware, anti-phishing, and more. Retina Scan on Connect protects the corporate network by evaluating the level of risk posed by each mobile and remote machine as it tries to connect and limits access based on security policies. As a result, organizations benefit from comprehensive protection from known and undefined vulnerabilities, the ability to patch during normally scheduled maintenance windows, enforcement of policy compliance and the ability to control access to the corporate network based on threat level.

About BeyondTrust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world’s 10 largest banks, seven of the world’s 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in Carlsbad, California. For more information, visit beyondtrust.com.