Modern Threats Attack from Client to Cloud

Today’s computing environment is more dangerous than ever. Modern threats take advantage of the increasing attack vectors presented by the explosion of interactions users have with personal and business data, devices, and applications. Today’s malware often uses very stealthy techniques, which conceal their malicious code, often going undetected until damage has been done.

• **Users unknowingly click** on malicious websites that transmit stealthy malware.

• **Sophisticated viruses get delivered** in e-mails and sleep until they’re triggered to wake.

• **Smart bugs exploit** an undiscovered zero-day vulnerability and propagate.

• **Attacks steal identities** or fake them, hijacking sessions and transactions.

• **Invading code sets up** before the OS launches, compromising the environment before an application is even started.
McAfee research has shown that all threats follow four unique phases of attack (Figure 1). Each phase requires specific technologies to detect, protect, and eradicate invading malicious code.

Rootkits are only one of the stealthy ways to conceal malware, but they are a favorite of cyber-criminals. On average, McAfee detects 1,200 new rootkits every day. Many rootkits dig in below the OS where anti-virus software can’t reach them.

Since these malware cannot be seen by the OS (and anti-virus software), companies need more powerful methods than today’s – even sophisticated – virus-detection software to protect a wider range of business clients against malicious attacks. McAfee and Intel security technologies and solutions work at the deepest levels of the business client – beyond the OS – to protect company assets.

McAfee and Intel – Joint Approach to Security

McAfee and Intel have joined forces against malware in order to ensure all users have engaging and productive computing experiences. To this end, they have devised much more effective ways to protect business clients against intrusions from security breaches and malware.

McAfee and Intel, leaders in security and silicon technologies, are uniquely capable to deliver advanced security solutions under the McAfee® Security Connected Framework. Together, their solutions enable a deeper level of security beyond the OS.

- Their joint software and hardware expertise lead to deeper protection for home and business PCs.
- With their world-class labs adding innovative research and development, they anticipate continually bringing new jointly developed solutions to market.

McAfee and Intel security solutions bring fresh innovation to secure the future of computing and the Internet.

**Advanced Detection and Prevention**

Detecting and preventing sophisticated malware at every phase of attack requires a multi-layered approach from within the silicon, beyond the OS, in the business client, and across the enterprise (Figure 2).

- Protection built into the silicon of business clients based on 3rd generation Intel® Core™ vPro™ processors and Intel® vPro™ technology
- Hardware-assisted security beyond the OS, using McAfee DeepSAFE™ technology and McAfee® Deep Defender
- Total endpoint security solutions from McAfee to protect data at every interaction
- Endpoint security management solutions to continually keep clients protected, including McAfee ePO™ Deep Command and McAfee Global Threat Intelligence™

---

**McAfee’s Security Labs Describes Malware Attacks**

Let’s face it, threats have gotten much more complex; like complex mechanisms they use multiple, consecutive methods to attack. At McAfee, our research teams continually analyze the threat landscape, and define threats in terms of their attack mechanisms, which consistently fall into four categories:

- **First Contact:** First, malware needs a way to come in contact with unsuspecting users.
- **Local Execution:** Second, they then use a diversity of ways to enter your system and begin to write files to disk and modify your system.
- **Establish Presence:** Third, they use several means to hide from detection before they even begin to do their dirty work of stealing personal information or scare you into buying useless security software.
- **Malicious Activity:** It’s not until the fourth phase that they really start to do their unscrupulous business.

---

**First Contact**

- Physical Access
- Unsolicited Message
- Malicious Website
- Network Access

How attacker first crosses paths with target

**Local Execution**

- Exploit
- Social Engineering
- Configuration Error

How attacker gets code running first time on target machine

**Establish Presence**

- Download Malware
- Escalate Privilege
- Persist on System
- Self Preservation

How attacker persists code on system to survive reboot, stay hidden from user and security software

**Malicious Activity**

- Propagation
- Bot Activities
- Adware and Scareware
- Identity and Financial Fraud
- Tampering

Business logic, what attacker wants to accomplish – steal passwords, bank fraud, purchase Fake AV

---

*Figure 1. Four phases of attack by malware*
Intel Built-in Security Technologies
The following security technologies are built into the silicon of business clients based on 3rd generation Intel Core vPro processors and Intel vPro technology:

- Intel® OS Guard: the next generation of Intel® Execute Disable Bit, protects against escalation of privilege attacks attempting to execute out of application memory space.
- Intel® Trusted Execution technology (Intel® TXT) establishes a hardware-based root of trust on a host, providing a known-good hosting environment. It helps ensure VMs only launch in a safe environment. Once launched, Intel TXT isolates VMs from other memory and cleans the memory when the VM shuts down, to prevent exposing its data to malware or other applications and environments.
- Intel® Virtualization technology (Intel® VT) provides specific security protection for executing processes (Intel VT-x) and isolation of virtual device memory space from other memory (Intel VT-d). In addition, Intel VT enhances virtual environment robustness and performance.
- Intel® Identity Protection technology (Intel® IPT) provides hardware-based identity protection by storing identity keys in firmware, out of reach of malware, rather than in software. Furthermore, Intel IPT provides a mechanism to ensure a real user, not malware, is entering authentication data, by bypassing system software during user input.
- Intel® Advanced Encryption Standard – New Instructions (Intel® AES-NI) accelerates encryption and decryption up to four times faster in McAfee® Endpoint Encryption, avoiding the ‘productivity/performance tax’ commonly associated with full encryption, and enabling ubiquitous encryption across business clients.
- Intel® Secure Key provides a hardware-based, clean source of random numbers for seeding encryption activities.
- Intel® Anti-theft technology (Intel® AT) uses embedded technology to self-protect data and the laptop on which it resides if the device goes missing. It can even enable the missing client to report its own location.

McAfee Business Protection Solutions
McAfee’s next-generation endpoint security platform offers the industry’s broadest protection for devices, data, and applications, along with the only unified management system available in the market. McAfee solutions provide enterprise-wide protection from chip to the Cloud.

- McAfee solutions for enterprise risk management and security compliance help minimize risk, automate compliance, and optimize security.
- Solutions for multiple business devices and services help protect server, desktop, laptop, mobile, and virtual environments; from chip to OS, databases, and the Cloud.
- McAfee’s next-generation, context-aware endpoint security with centralized policy management helps endpoints stay secure and comply with central security policies.

McAfee Complete Endpoint Protection
McAfee endpoint protection solutions unite industry-leading endpoint security and data protection with centralized management. Where McAfee products leverage Intel built-in technologies, McAfee security provides a deeper level of protection for business clients. The following is a small, but crucial, sampling of McAfee business client protection products.

McAfee DeepSAFE™ technology helps fundamentally change the security game. McAfee DeepSAFE, co-developed with Intel, sits below the OS and provides an unfettered view of system memory and a trusted view of system events, offering an entirely new vantage point on business client computing activities.

McAfee DeepSAFE technology allows McAfee to develop new hardware-assisted security products to take advantage of a “deeper” security footprint. For example, many advanced persistent threats (APTs) include stealth techniques, such as rootkits, that embed themselves deep below the OS and evade current security solutions. McAfee DeepSAFE technology enables new McAfee security products that can proactively detect and prevent stealthy APTs and malware.

McAfee DeepSAFE technology and 3rd generation Intel Core vPro processors combine the flexibility of software and power of hardware to deliver a new foundation for security.

McAfee® Deep Defender helps stop advanced stealth attacks with the industry’s first hardware-assisted security enabled by McAfee DeepSAFE technology. Unlike traditional security solutions that operate above the OS, Deep Defender operates beyond the operating system, providing real-time behavioral monitoring of low-level kernel operations to reveal and remove advanced, hidden attacks.

McAfee Deep Defender protects the business client before a rootkit has a chance to conceal its malware. Yet, it requires no prior knowledge of the rootkit to detect its existence. Deep Defender identifies malicious stealth behavior as it tries to execute, providing true zero-day protection.

Figure 2. Multi-layered security technologies approach with new McAfee software solutions enhanced by new built-in Intel silicon-based technologies
McAfee Endpoint Encryption for business clients safeguards data and minimizes compliance issues with transparent encryption and strong access control. McAfee Endpoint Encryption leverage Intel AES-NI to accelerate encryption and decryption of files, folders, and entire disks without a productivity/performance penalty.

The McAfee Security Management solution helps reduce the costs of security and IT management with comprehensive and hardware-assisted management tools.

McAfee ePolicy Orchestrator® (McAfee ePO) is the foundation of the McAfee Security Management Platform, which unifies management of endpoints, networks, and data for risk and compliance management, policy setting and enforcement, and security event monitoring and remediation.

McAfee ePO™ Deep Command uses Intel vPro technology to deliver endpoint security management beyond the OS, reducing security operations costs, while enhancing an organization’s security posture. McAfee ePO Deep Command enables IT security management to control powered-off business clients and servers, execute security tasks – including updates, deployments, and configuration changes – and perform remote remediation of computers with disabled operating systems.

McAfee Global Threat Intelligence™ (McAfee GTI) offers the most comprehensive threat intelligence in the security market. McAfee GTI gives McAfee visibility across all threat vectors – file, web, message, and network – plus a view into the latest vulnerabilities across the IT industry. McAfee GTI correlates real-world data collected from millions of sensors around the globe. It delivers real-time, and often predictive, protection via its security products to business clients, servers, virtual environments, and more.

Conclusion

Companies need advanced business client security solutions. When malicious code attempts to dig in, McAfee and Intel technologies, working in the silicon and beyond the OS, can quickly detect and prevent these assaults. McAfee and Intel are uniquely capable of providing these advanced solutions with leading technologies and research and development. From authentication to encryption to inspection to trust, a company’s most effective protection against stealthy malware comes from McAfee and Intel solutions built into the silicon, enabled by hardware-assisted technologies, and delivered using advanced endpoint protection and management software.