



# Check Point Integrity\* and Intel® Active Management Technology

<b>Company</b>	Check Point Software Technologies, Ltd. is a worldwide leader in securing the Internet. It is a market leader in the worldwide enterprise firewall, personal firewall and virtual private network (VPN) markets.
<b>Business Challenge</b>	Respond immediately to Day Zero and other network threats providing protection for machines, even when they are powered off or their operating systems are unavailable.
<b>Technology Solution</b>	Check Point Integrity*
<b>Enabled By</b>	Intel® Active Management Technology (Intel® AMT)

## Drastically Reduce Response Time and Establish Immediate Protection Against Network Threats

Information technology (IT) managers have two primary security goals: to proactively prevent security threats and to resolve threat outbreaks as quickly as possible with minimal business disruption. Now new hardware capabilities enabled by Intel Active Management Technology (Intel AMT), coupled with Check Point Integrity\* endpoint security, empower administrators to issue immediate security policy changes to PCs—even those that are powered off or otherwise unavailable. Using Integrity, administrators can restrict or quarantine PC network access as soon as a threat is detected. Protection for Intel AMT-enabled PCs is nearly immediate, closing the window of vulnerability.

### Today's Challenge

IT managers usually have predefined security policies and procedures in place when declaring a network security emergency. A basic network emergency might require client machines to disable email access, or to block file sharing while allowing domain name servers (DNS) access. In more serious scenarios, clients may only be allowed dynamic host configuration protocol (DHCP), thus restricting their overall network exposure. Finally, the most serious threats may require a full client quarantine to protect all machines until IT has resolved the potential problem.

IT departments have traditionally experienced two delays in issuing instructions during a network emergency. First, emergency broadcasts were only received when the client contacted the server for an update. While this may take only a few minutes, each one of those minutes is crucial. The second delay occurred when machines were powered down or otherwise unavailable. When those machines were subsequently powered up, they would be vulnerable until they obtained a policy update.

### The Solution: Check Point Integrity and Intel AMT

Using Check Point Integrity to secure Intel AMT-enabled systems now gives IT managers enhanced capabilities to immediately protect machines even when systems are powered down. When a worm or virus outbreak occurs, the IT department has a window of opportunity—often as short as 5 or 15 minutes—in which to decide how to deal with the threat before it becomes widespread. During that window, the security threat containment strategy needs to be developed and then deployed as rapidly

as possible to minimize the amount of time in which the corporation's computers are vulnerable. Integrity is taking advantage of the Intel AMT nonvolatile storage and out-of-band (OOB) communication capabilities to store policy updates locally on the PC and dramatically reduce that window of vulnerability. As soon as IT managers become aware of a threat, they can now immediately issue a network emergency broadcast to all Intel AMT clients. Instructions are written into the Intel AMT nonvolatile memory, whether those machines are powered on or off, and Integrity will—immediately or when the client next powers up—restrict access to certain PC ports, segments of the network, and even communication protocols. In the worst-case scenario, clients can be quarantined completely.

### Enhanced Protection with Nonvolatile Memory

A typical mid-size enterprise might have employees spread across geographic locations, stretching IT resources thin. Check Point Integrity and Intel AMT offer these enterprises a unique advantage in controlling and protecting their endpoints. For example, an IT manager in California might be awakened in the middle of the night because a worm has broken out in the U.K. office. The IT manager could declare an immediate network emergency to preserve the overall network integrity as her team decides how to stop the worm. Security policies sent to all Intel AMT-enabled machines in the U.S., even those powered off for the night, ensure that the enterprise is secured. For IT, using Integrity for Intel AMT clients allows a rapid but measured response.

As U.S. employees start their work day and power up their machines, Integrity launches prior to network access, and checks the Intel AMT persistent memory for any policy changes, including whether network access should be allowed, and at what level. If a network emergency is in effect, Integrity enforces the instructions found in the Intel AMT nonvolatile storage. In the previous example, access to the European office would be restricted, users would be notified of the change in policy, and the U.S. machines would be protected until the threat is fully resolved.

### Greater Visibility of Endpoints

Intel AMT also enhances IT's visibility of endpoints. Traditionally, devices are identified using a media access

control (MAC) address or other identifier installed by the IT department. For Intel AMT-enabled systems, Integrity can now use the unique hardware machine identifier (ID) of each AMT device to mark it eligible for a network emergency update. This ID is stored in the Intel AMT nonvolatile memory and can be accessed whether the machine is on or off. Administrators can now quickly and accurately identify all Intel AMT devices on the network, initiate a network emergency to protect that population of endpoints, and then proceed to focus on securing the remaining endpoints.

## Summary

Intel AMT-enabled systems coupled with Check Point Integrity empower IT managers to respond rapidly to threat outbreaks, with powerful, easy-to-use controls for restricting or locking down endpoint network access. Response time no longer depends on the power state of a machine. IT managers now have a distinct advantage in crafting a graceful resolution which minimizes business disruption and end-user angst. Check Point Integrity used with Intel AMT-enabled systems offers a fast, always-available mechanism to secure endpoints and to preemptively protect against Day Zero threats.

### Solution Benefits

Dramatically reduces response time to Day Zero threats and other threat outbreaks.

Secures endpoints whether they are powered on or off.

Lowers the total cost of ownership (TCO) of the computing environment.

## For More Information

Intel AMT enables software vendors to deliver both enhanced and new IT solutions that make network management easier and reduce the overall cost of managing computing environments.

**For more information about Intel AMT, visit**  
[www.intel.com/go/iamt](http://www.intel.com/go/iamt)

**For more information about Check Point Integrity endpoint security, visit**  
[www.checkpoint.com/products/integrity/](http://www.checkpoint.com/products/integrity/)

