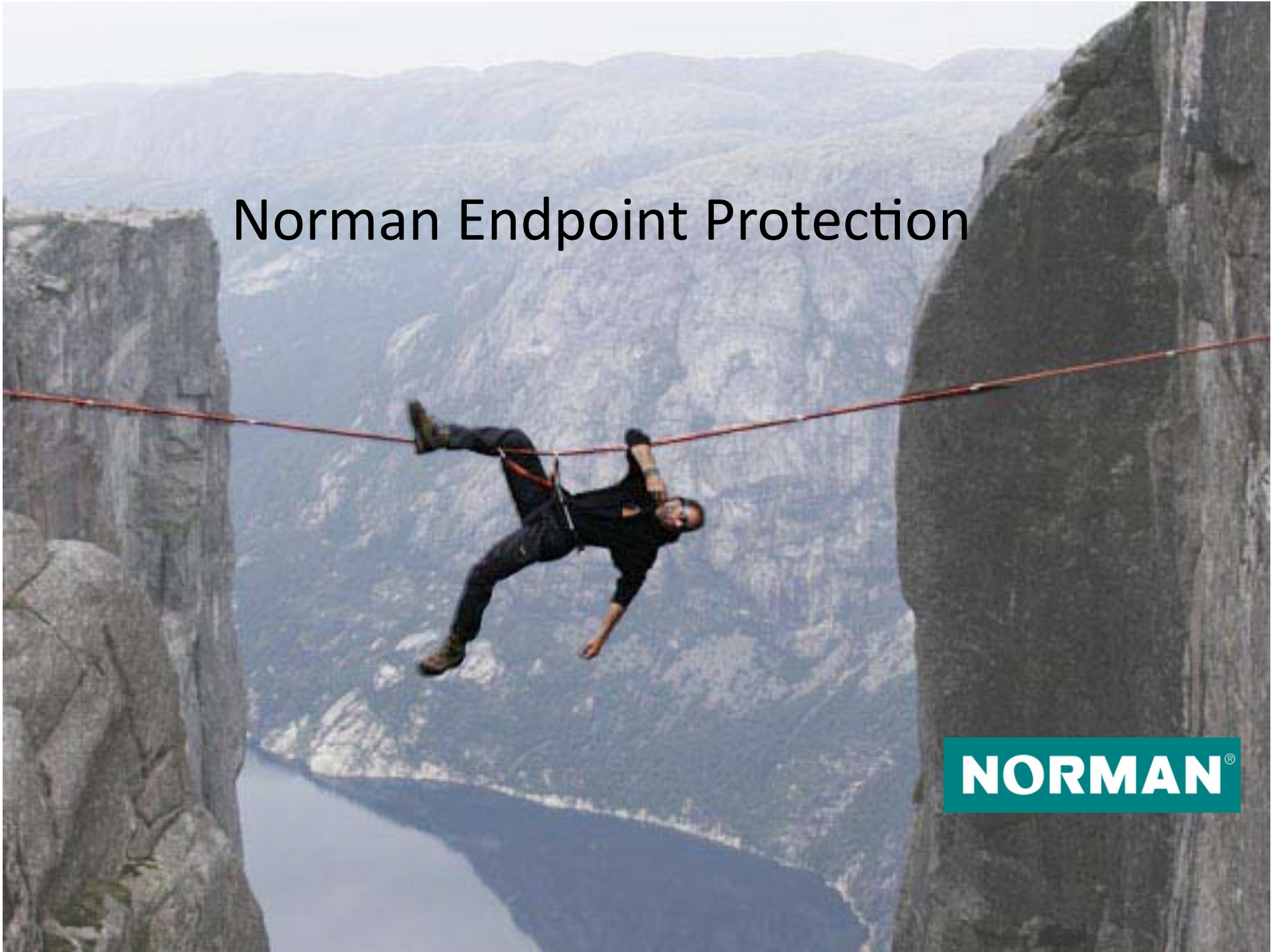


Norman Endpoint Protection

NORMAN[®]



What is Norman Endpoint Protection (NPRO)?

Proactive network security for corporate networks and mobile workforces. It protects against malware with:

- Powerful detection technologies
- Easy-to-use management console
- Scalability and passive technology for small footprint

NPRO protects the network with four powerful technologies:

- Norman Endpoint Manager
 - Norman Exploit Detection
 - Norman DNA Matching
 - Norman Sandbox Technology
-



SAFETY FIRST

NORMAN®

Why do you need NPRO?

Businesses of all sizes are vulnerable to malware attacks due to:

- Increasing workforce mobility
 - Collaboration with outside partners and vendors
 - Increase of information from a variety of sources flowing through the network
 - Proliferation of Web technologies
 - Sophisticated malware that is more damaging and prevalent than ever before
-



SAFETY FIRST

NORMAN®

A new generation of malware

Today's generation of sophisticated malware damages businesses through:

- Reduced productivity
- Lost confidential information
- Stressed IT resources
- Lost customers
- Lower revenues

Malware is spread over multiple endpoints including Bluetooth devices, iPods and USB drives.

According to the FBI, cyber crime is now larger than the worldwide narcotic market.

Source: U.S. Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, June 2007.

The malware landscape has changed

Several factors have changed the way hackers operate:

- Viruses that once made headlines are now silent and often go unnoticed
- Threats that once put anyone, anywhere at risk are now highly targeted by professional cyber criminals
- Malware developer tools are now available on the Internet, allowing novices to create security threats
- Inadvertent downloading exposes sensitive corporate data simply because employees don't know any better



SAFETY FIRST

NORMAN®

The threat is real

In 2008, the W32/Conficker virus infected as many as 10 million computers and continues to spread. Clean-up costs exceeded \$9.1 billion.

The W32/Virut family of highly polymorphic viruses was among the top 5 malware threats in 2009.

Proactive next-generation network security solutions like Norman Endpoint Protection are more critical than ever before.

Source: Reuters News Service, *Cyber Secure Institute Issues Analysis of Conficker Controversy*, April 21, 2009.

Today's detection technologies

Exact detection identifies known malware and blocks it with exceptional accuracy. However, it only protects against known threats that have been profiled. So it must be combined with other methods.

Generic detection identifies key characteristics from malware family samples and creates a generic detection rule. While exact detection may initially identify a new threat, more generic detection rules will combat variations of the new malware family.

Norman Endpoint Protection uses exact and generic detection methods to block existing and new malware from infecting a network.



SAFETY FIRST

NORMAN®

Norman Endpoint Protection technologies

Norman Endpoint Protection provides powerful proactive security by combining several technologies:

- Norman Endpoint Manager
- Norman DNA Matching
- Norman Exploit Detection
- Norman Sandbox



SAFETY FIRST

NORMAN®

Norman Endpoint Manager (NEM)

Norman Endpoint Manager is a powerful, easy-to-use central management tool that includes:

- Web-based graphical application
 - Passive discovery technology to detect all IP-based devices in the network
 - Security-level indicator to provide a quick view of the security state of the network
 - Built-in policy engine to provide a simple, centralized interface to monitor and configure network clients
-

Norman Endpoint Manager (NEM), cont.

Norman Endpoint Manager performs several functions:

- Provides a view of network devices and their status
 - Generates and displays event and status statistics
 - Manages incoming alarms, warnings and errors
 - Manages administrators, policies and configurations and assigns them to client groups
 - Manages product installation and the Internet update configuration
 - Provides redundancy for the topology and configuration database
 - Generates and exports reports from statistics
 - Serves as a distribution point for definition files and software updates
-



SAFETY FIRST

NORMAN®

NEM: Security-level indicator

Norman Endpoint Manager's security-level indicator provides a quick view of the security state of the network.

It calculates risk based on weighted analysis of errors, warnings, alarms and locations of various clients within a 24-hour period.

Any malware incidents, outdated clients or system warnings will change the indicator and report detailed incident information.



SAFETY FIRST

NORMAN®

NEM: Policy-based engine

Norman Endpoint Manager's policy-based engine allows administrators to intelligently deploy endpoints throughout a company's infrastructure.

It allows IT to perform administrative tasks such as:

- Manage clients on the network
 - Distribute and install software
 - Establish policies and settings
 - Run reports
-



SAFETY FIRST

NORMAN®

Norman DNA Matching

All malware is made up of computer code DNA building blocks.

Since authors of malware reuse these programming codes, Norman DNA Matching can identify and stop new forms of malware based on their malicious DNA.

Signature methods cannot do this as they can only match malware that has previously been profiled.

Norman Exploit Detection

Many types of malware infect networks by targeting vulnerabilities in popular applications and file formats.

Norman Exploit Detection identifies malware by:

- Inspecting common file types (PDF, MS Office, Flash, etc.)
 - Looking for shellcode that issues unwanted commands
 - Evaluating shellcode for criteria not present in legitimate programs
 - Identifying the behavior of malware in that file format
-



SAFETY FIRST

NORMAN®

Norman Sandbox Technology

Norman Sandbox Technology stops new, unidentified malware. In a simulated environment, it:

- Analyzes and identifies malicious code before it infects the network
 - Simulates the computer, hard drive, memory, operating system, network and Internet
 - Works in real time without slowing down the network
 - Detects many types of viruses including those spread locally and those spread over the Internet (e.g., binary malware, network worms, etc.)
 - Protects against malware that targets SMTP, News, IRC and DNS
-



SAFETY FIRST

NORMAN®

Conclusion

Norman Endpoint Protection exceeds the weaknesses of traditional security solutions by delivering:

- Proactive, centralized protection for all devices
- Easy, intelligent client configuration
- Protection against all potential security risks, old and new
- Flexibility, scalability and advanced performance

Norman Endpoint Protection provides the sophisticated technology businesses need to protect their valuable networks while conducting business as usual with complete peace of mind.



SAFETY FIRST

NORMAN®

About Norman

Norman ASA is a world-leading company within the field of data security, Internet protection and analysis tools. Through its SandBox technology, Norman offers unique and proactive protection unlike any other competitor. While focusing on its proactive antivirus technology, the company has formed alliances which enable Norman to offer a complete range of data security services. Norman was established in 1984 and is headquartered in Norway with a presence in continental Europe, the U.K. and the U.S.

*For more information about Norman Endpoint Protection,
please visit <http://www.norman.com>.*
