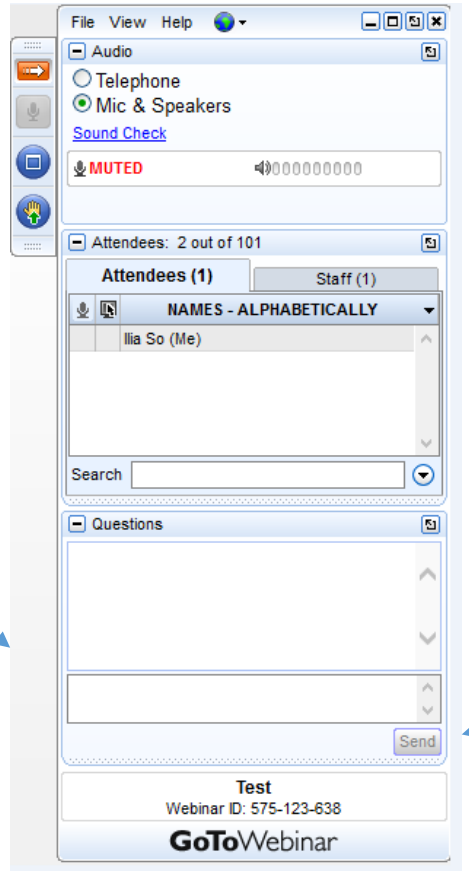
Outsmarting Ransomware: Hints and Tricks

Netwrix Corporation
Bob Cordisco
System Engineer

How to Ask Questions

Type your question here

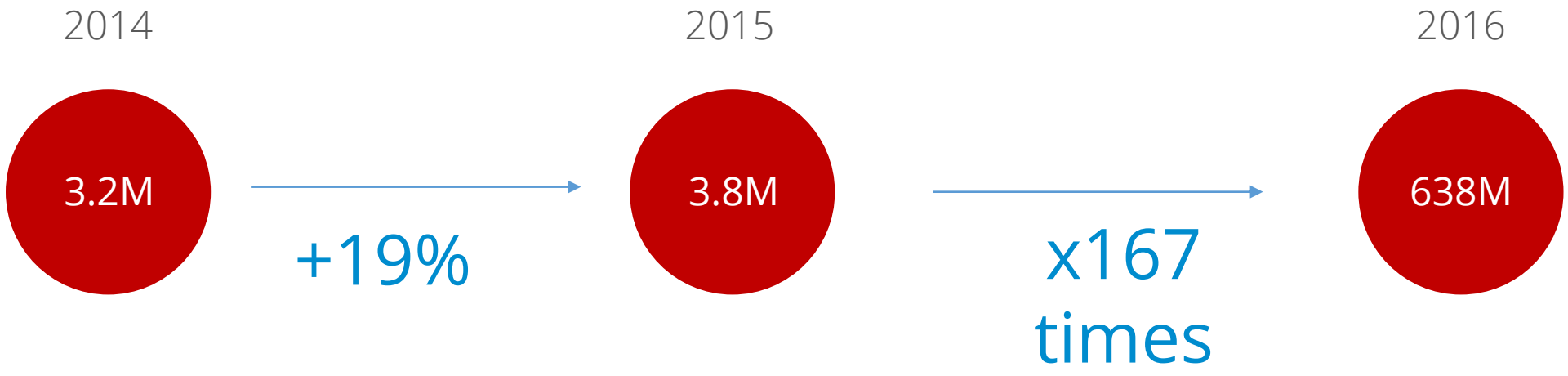


Click “Send”

Agenda

- Ransomware Trends
- 9 Hints and Tricks: How to Outsmart Ransomware
- Demonstration

The Rise of Ransomware



$1B in ransom fees paid in 2016

Ransomware News

- Maersk loses $300M due to NotPetya ransomware attacks
- The ‘big return’ of Mamba ransomware in Saudi Arabia and Brazil: Remember San Francisco Municipal Transportation Agency attack in November?

‘The Week in Ransomware’ weekly updates: https://www.bleepingcomputer.com/

Hint #1: Know How It's Delivered and Executed

WannaCry, Petya, etc.

- Are ransomware cryptoworms
- Use ETERNALBLUE
- Leverage the Microsoft Windows file-sharing vulnerability
- Target unpatched Windows
- Demand ransom: $300+ (in bitcoins)
- WannaCry 2.0 comes without killswitch

Locky, Cryptolocker, etc.

- 97% of phishing emails in 2016 delivered ransomware
- Average price for individuals: $500
- Average price for companies: $17000+

Hint #2: It's Time to Talk to Your Email Hygiene Provider

Ask your e-mail hygiene provider to enable their URL scanning protection!

Provider replaces the links in emails with a link to the portal

A user clicks a link

The provider examines target destination

Warning 'Don't Proceed' is displayed

Hint #3: Make sure EternalBlue Exploit Is Closed for You

1. Disable SMBv1 on your Windows servers by running this PowerShell cmdlet: Remove-WindowsFeature FS-SMB1

Note: A restart will be required after executing this command.

2. Make sure that you have applied the MS patch (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx) to your infrastructure.
3. Add rules on your AV to prevent the creation of .wnry file extensions.
4. Block TCP ports 139 and 445 from allowing inbound Internet connections.
5. Whitelist these domains (as WannaCry checks them) to stop the attack:

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Note: This only works for direct connections; if using a proxy (as on enterprise networks), it won't work.

6. Educate users about the WannaCry ransomware threat and explain how not to fall victim to phishing attacks.
7. Set up alerts for WannaCry threat patterns (http://get.netwrix.com/get_alerts_on_wannacry_attacks_lf/).
8. Pray.

Hint #4: Enable Least Privileged Principle

- Deploy role-based access controls and group policies
- Segment the network into VLANs
- Setup unique accounts for users' administrator and non-administrator activities
- Perform regular audits of employee accounts to identify changes in roles
- Patch software regularly

Hint #5: Configure Group Policy Properly

- Enable display of file extensions
- Blacklist all applications from running on workstations and granularly whitelist only trusted ones
- Block executable extensions
- Block AutoPlay to disable software execution from removable media

Hint #6: Make Sure You've Done This

- Block macros from running in Office files from the Internet.
- Properly configure your web filter, firewall and antivirus software to block access to malicious websites
- Blacklist TOR IP addresses
- Set .JS files to open with Notepad by default
- Configure your firewall to whitelist only the specific ports and hosts you need
- Segregate your network into different zones with unique access to each
- Create a guest network for new or unknown equipment
- Look for spikes in file modification activity

Hint #7: Setup a Honeypot Using FSRM

- Create a share with a $ in front of the name (using File Server Resource Manager)
- Let the group Authenticated Users have full control of this share
- Cut off user's access when the FSRM file screen notices write activity

Get-SmbShare -Special $false | ForEach-Object { Block-SmbShareAccess -Name $_.Name -AccountName '[Source Io Owner]' -Force }

Hint #8: Call for Help

Learn more:

http://nomoreransom.org

- Crysis
- Marsjoke
- Polyglot
- Wildfire
- Chimera
- Teslacrypt
- Shadecoinvault
- Rannoh
- Rakhni

Hint #9: Just One More Thing to Remember

- Back up!
- Always install latest patches and updates
- Beware of pseudo-crypto-ransomware pop-ups
- Educate your employees and executives! Send them the Ransomware Survival Guide: https://www.netwrix.com/download/documents/Ransomware_Survival_Guide.pdf

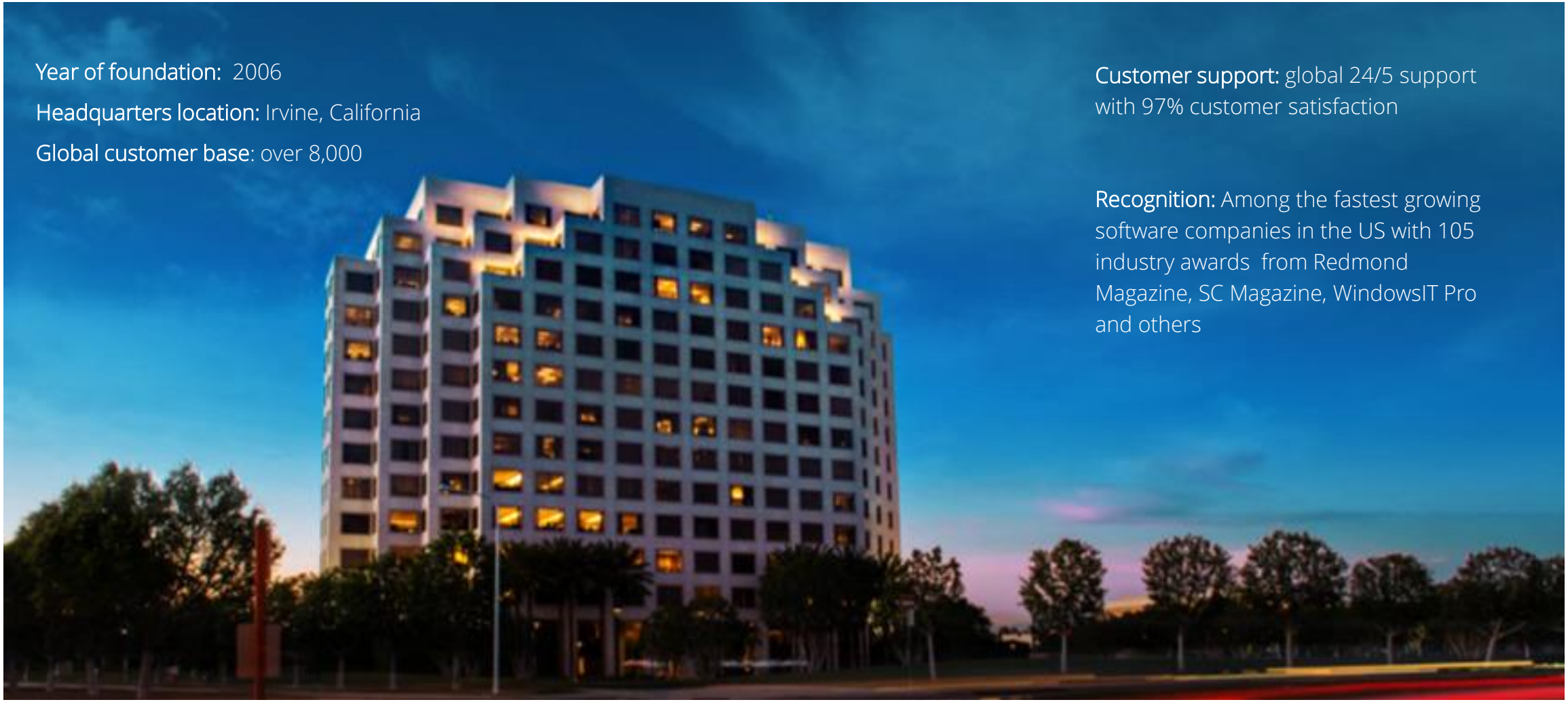
Netwrix Auditor

Demonstration

Netwrix Auditor Applications

- Netwrix Auditor for Active Directory
- Netwrix Auditor for Azure AD
- Netwrix Auditor for Exchange
- Netwrix Auditor for Office 365
- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for EMC
- Netwrix Auditor for NetApp
- Netwrix Auditor for SharePoint
- Netwrix Auditor for Oracle Database
- Netwrix Auditor for SQL Server
- Netwrix Auditor for Windows Server
- Netwrix Auditor for VMware

About Netwrix Corporation



Netwrix Customers

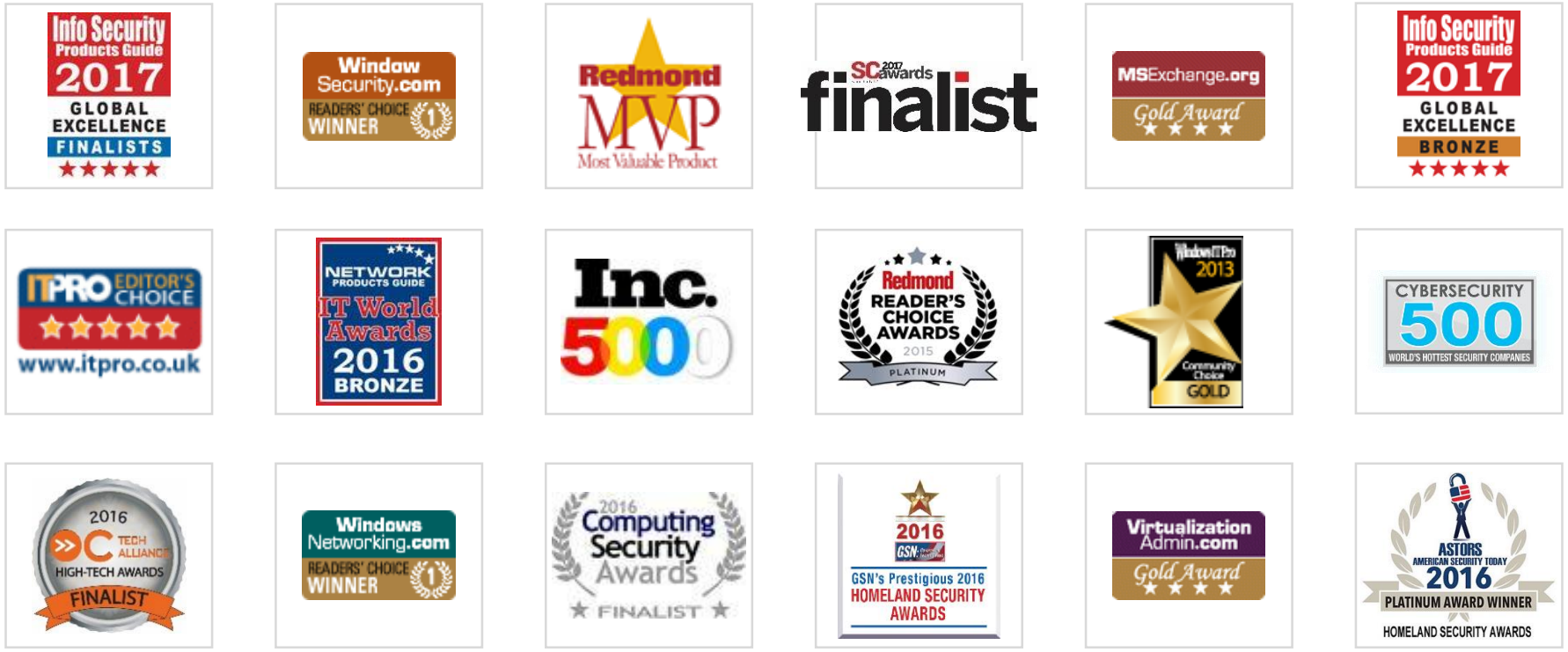
Financial

Healthcare & Pharmaceutical

Federal, State, Local, Government

Industrial/Technology/Other

Industry Awards and Recognition



All awards: www.netwrix.com/awards

Next Steps

Free Trial: setup in your own test environment:

- On-premises: netwrix.com/freetrial
- Virtual: netwrix.com/go/appliance
- Cloud: netwrix.com/go/cloud

Test Drive: run a virtual POC in a Netwrix-hosted test lab netwrix.com/testdrive

Live Demo: product tour with Netwrix expert netwrix.com/livedemo

Contact Sales to obtain more information netwrix.com/contactsales

Webinars: join our upcoming webinars and watch the recorded sessions

- netwrix.com/webinars
- netwrix.com/webinars#featured

Thank You!