



SECURING REMOTE ACCESS

Basic & Advanced Strategies

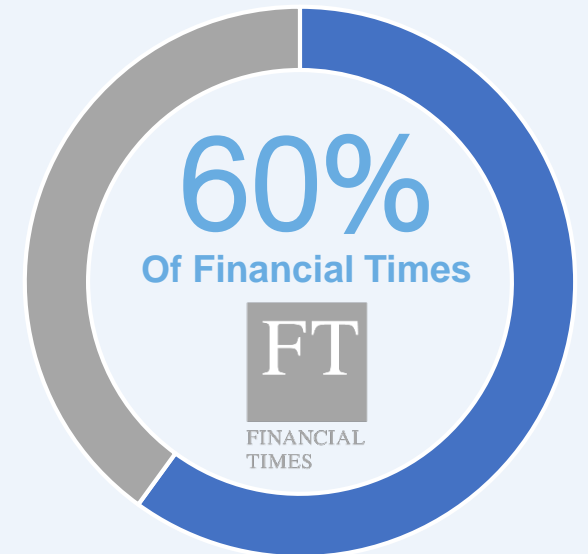
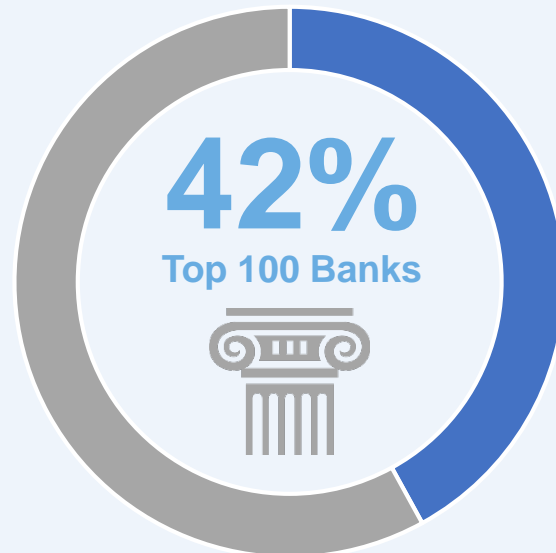
February 2019



Sam Heiney

Global Product Solutions Director

sam.heiney@netop.com



Securing Remote Access

- Lessons from 2018
- Best Practices & Advanced Strategies
- Questions

Lessons From 2018: Who



Retailers remain the biggest target

17% of
all data
breaches



Attacks on Service Providers Increased

9% of all
data breaches

Compromises of service providers often enabled most remote access attacks ... Often, the attacker gained remote access to multiple locations by obtaining service-provider remote access credentials, either by compromising the service-provider network (and thus VPNs) or by simply obtaining default passwords in cases where remote access tools were internet accessible.

-Trustwave Global Security Report 2018

Lessons From 2018: What



Payment Card Data is
the objective

42%
of retail
breaches



P.I.I. has become
more valuable

10%
increase from
2017

Lessons From 2018: How

#1

Phishing is the top
attack vector

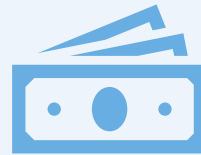
47%
of retail
breaches



Remote Access is the
method of choice

23%
of retail
breaches

Lessons From 2018: Cost



Average cost of a data
breach in 2018:

\$3.86
Million

Best Practices and Advanced Strategies

- Access
- Authentication
- Authorization
- Logging

Best Practices & Advanced Strategies:

Access



BASIC

- Endpoint protection
- Encryption
- Minimize threat vectors (RDP, VNC)



ADVANCED

- Virtualization
- IP/MAC Filtering
- Secure deployments

Best Practices & Advanced Strategies: Authentication



BASIC

- Directory Services Integration
- Password Management
- MFA



ADVANCED

- PAM
- Context specific controls

Best Practices & Advanced Strategies: Authorization



BASIC

- Individual or group permissions



ADVANCED

- Role-based permissions
- Device groups
- Granular permissions
- Application whitelisting

Best Practices & Advanced Strategies: Logging



BASIC

- Who
- What
- When



ADVANCED

- Screen recording
- Custom logging
- Unalterable audit logs

Summary: Best Practices & Advanced Strategies

ACCESS

AUTHENTICATION

AUTHORIZATION

LOGGING



BASIC

- Endpoint protection
- Encryption
- Minimize threat vectors (RDP, VNC)



BASIC

- Directory Services Integration
- Password management
- MFA



BASIC

- Individual or group permissions



BASIC

- Who
- What
- When



ADVANCED

- Virtualization
- IP/MAC Filtering
- Secure deployment



ADVANCED

- PAM
- Context specific controls



ADVANCED

- Role-based permissions
- Device groups
- Granular permissions
- Application whitelisting



ADVANCED

- Screen recording
- Custom logging
- Unalterable audit logs

Download the Workbook



<https://nrc.netop.com/download-securing-remote-access-workbook>