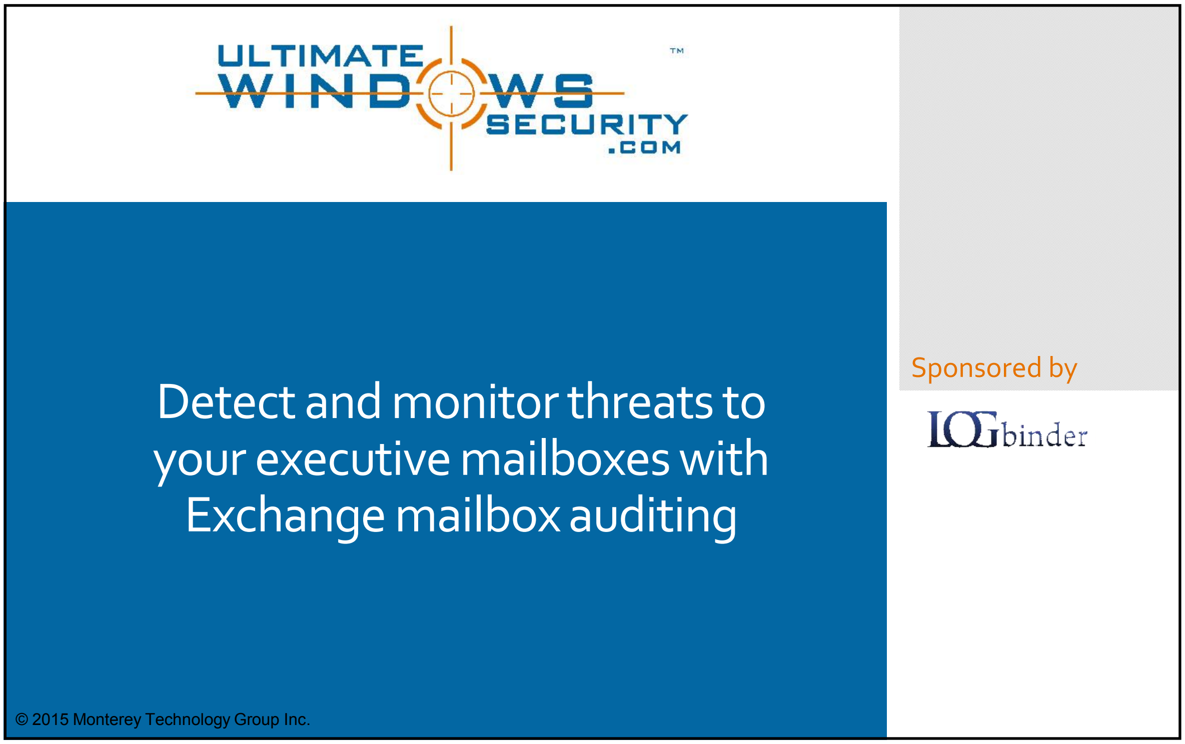
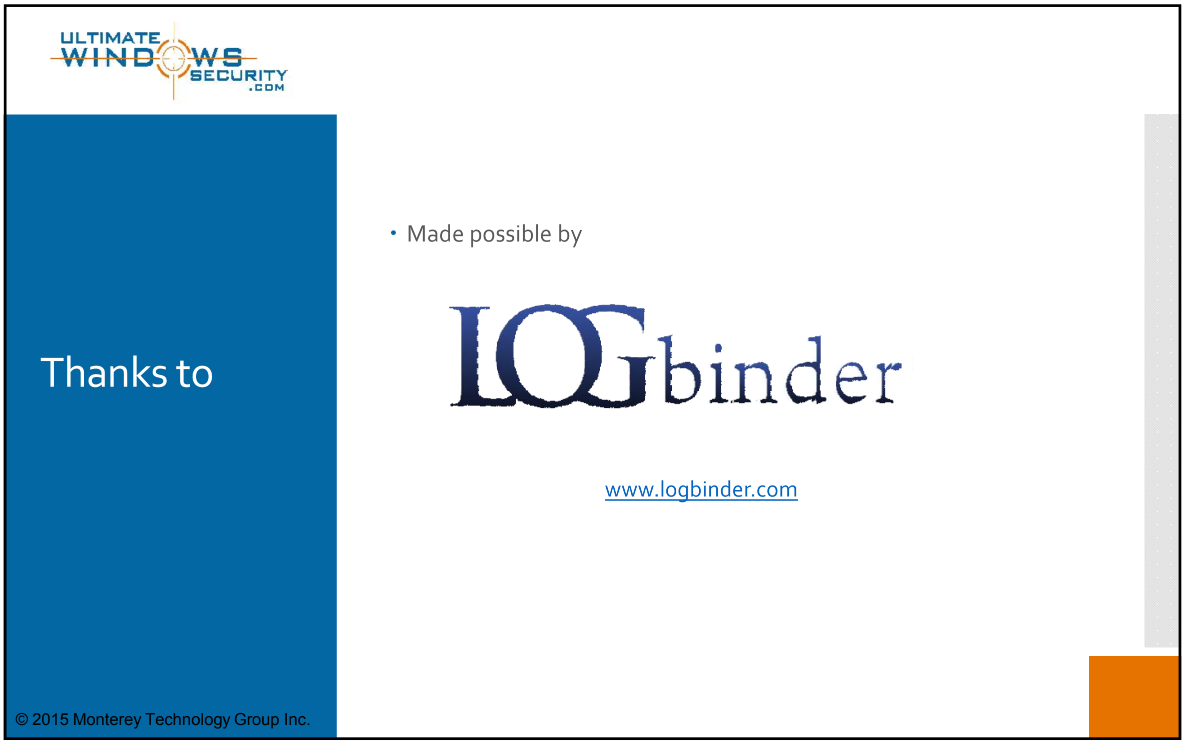


ULTIMATE WINDOWS SECURITY.COM ™

Detect and monitor threats to your executive mailboxes with Exchange mailbox auditing

Sponsored by

LOGbinder



ULTIMATE WINDOWS SECURITY.COM

Thanks to

- Made possible by

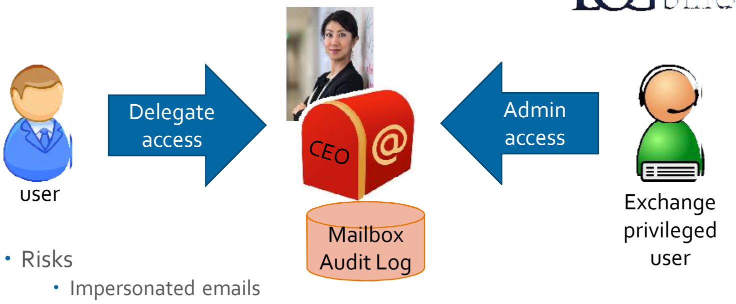
LOGbinder

www.logbinder.com

Preview of Key Points

- Auditing Exchange mailboxes
  - How to enable
  - What you can audit
  - How to access log
  - Important things to understand
- Managing audit policy
- Complexity of getting Exchange audit logs into your SIEM
- The Exchange bug
  - Prevents timely detection of non-owner mailbox access
  - What we (LOGbinder) are doing about it

Executive mailboxes



user

Delegate access

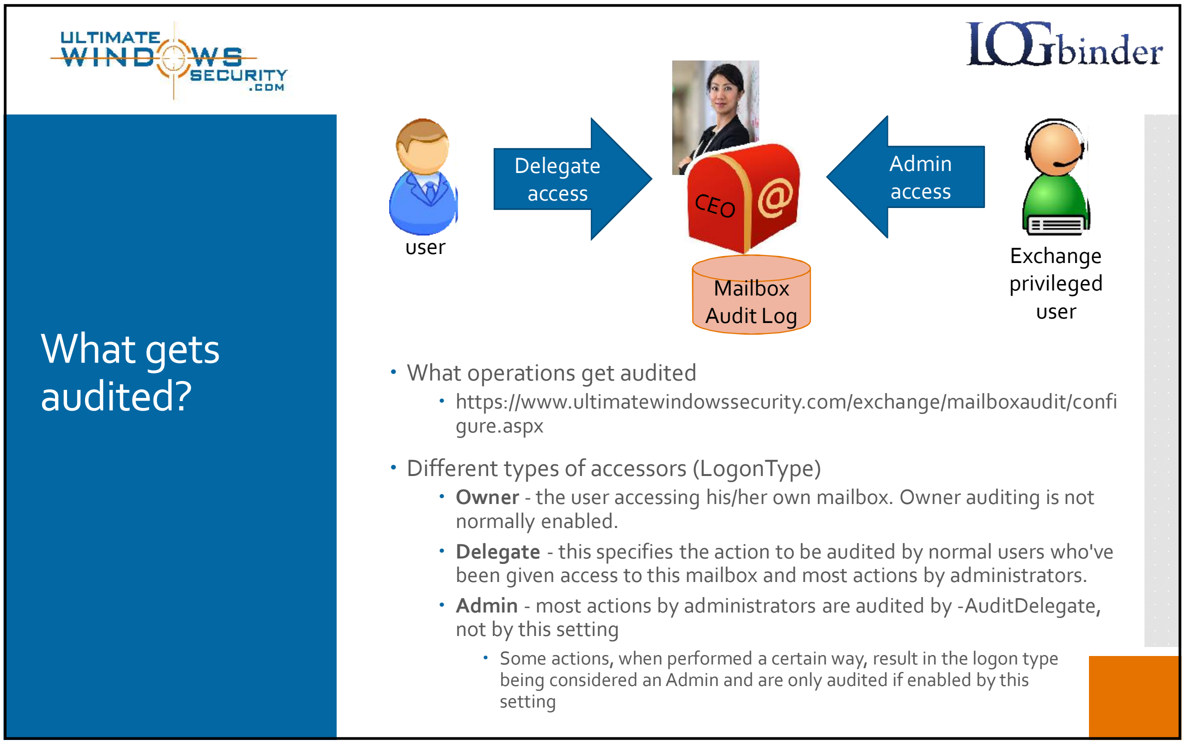
CEO @

Mailbox Audit Log

Admin access

Exchange privileged user

- Risks
  - Impersonated emails
  - Business plans leaked
  - Embarrassing corporate incidents leaked
  - Information grabs
  - Industrial espionage
  - Customer/patient information
  - Internal reports
  - Competitive analysis
  - Trade secrets
  - Product designs
  - …



What gets audited?

user

Delegate access

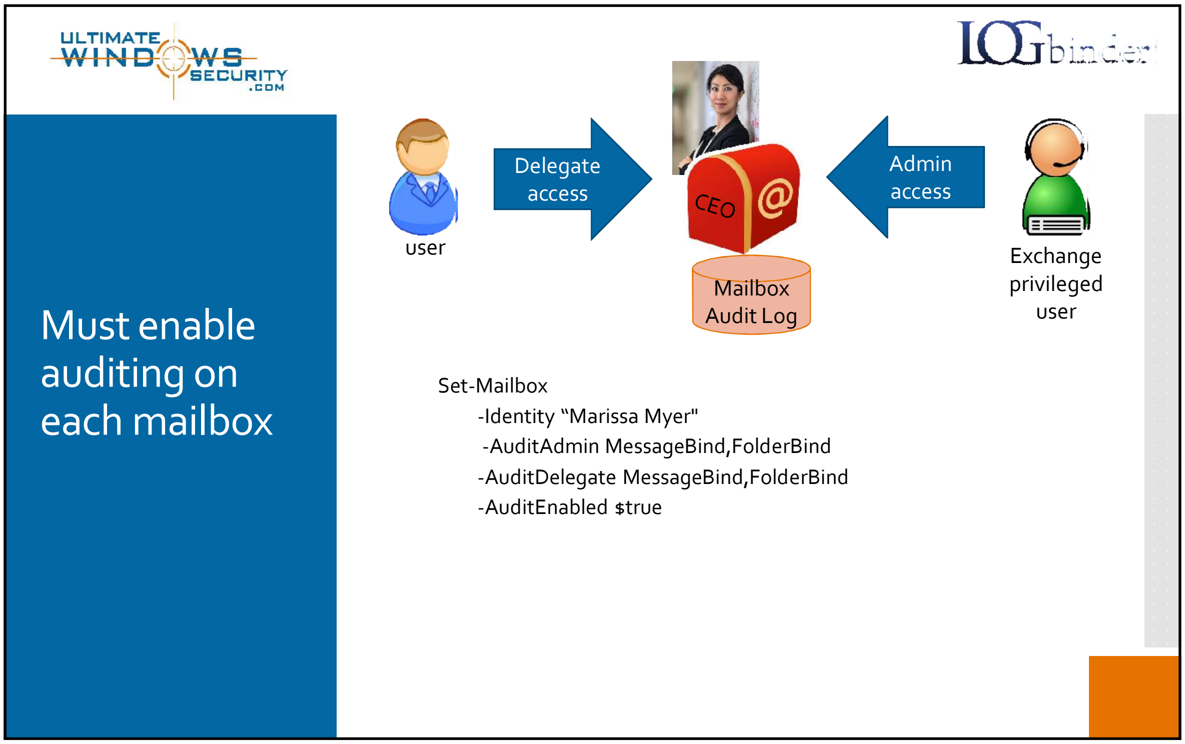
CEO

Mailbox Audit Log

Admin access

Exchange privileged user

- What operations get audited
  - https://www.ultimatewindowssecurity.com/exchange/mailboxaudit/configure.aspx
- Different types of accessors (LogonType)
  - **Owner** - the user accessing his/her own mailbox. Owner auditing is not normally enabled.
  - **Delegate** - this specifies the action to be audited by normal users who've been given access to this mailbox and most actions by administrators.
  - **Admin** - most actions by administrators are audited by -AuditDelegate, not by this setting
    - Some actions, when performed a certain way, result in the logon type being considered an Admin and are only audited if enabled by this setting



Must enable auditing on each mailbox

user

Delegate access

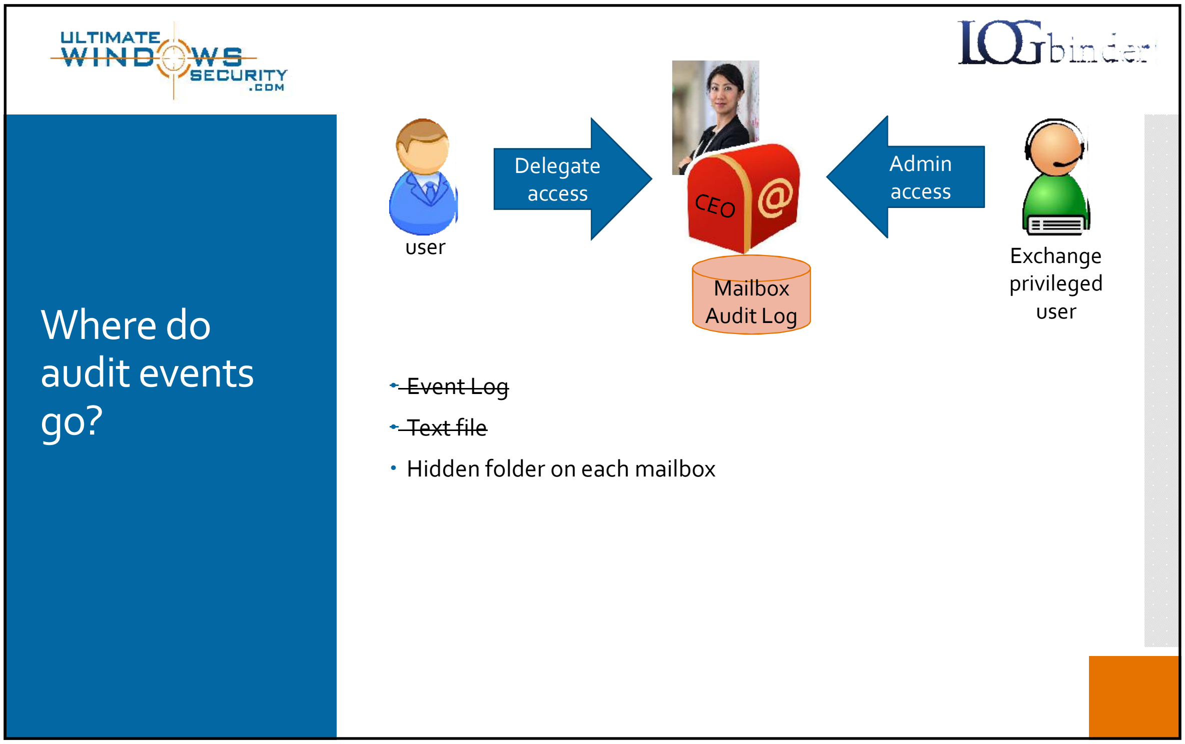
CEO

Mailbox Audit Log

Admin access

Exchange privileged user

```
Set-Mailbox
      -Identity "Marissa Myer"
       -AuditAdmin MessageBind,FolderBind
      -AuditDelegate MessageBind,FolderBind
      -AuditEnabled $true
```



Where do audit events go?

user

Delegate access

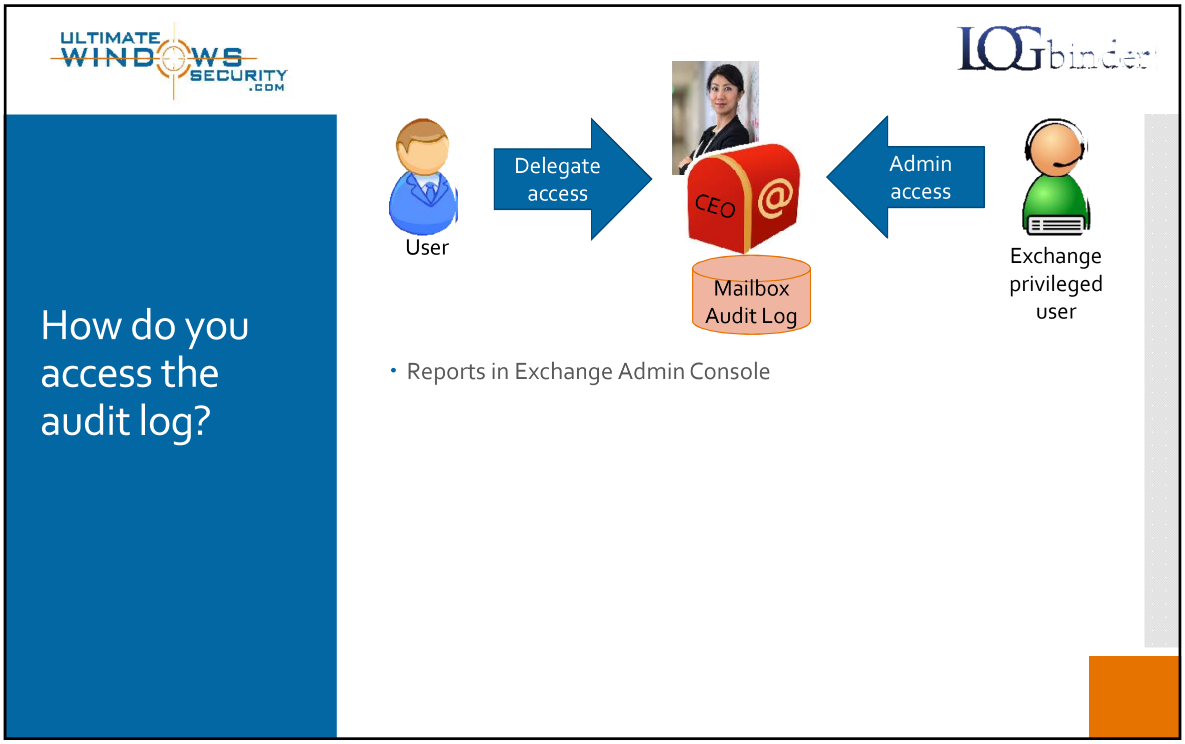
CEO

Mailbox Audit Log

Admin access

Exchange privileged user

- ~~Event Log~~
- ~~Text file~~
- Hidden folder on each mailbox



How do you access the audit log?

User

Delegate access

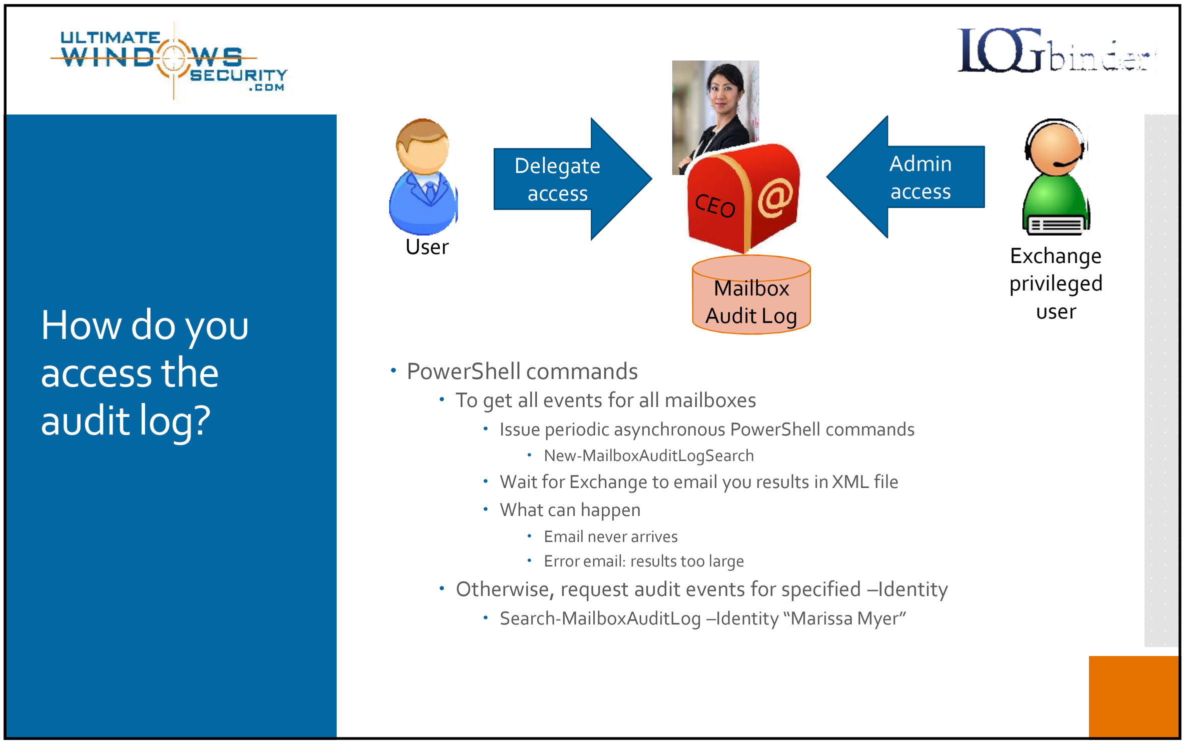
CEO

Mailbox Audit Log

Admin access

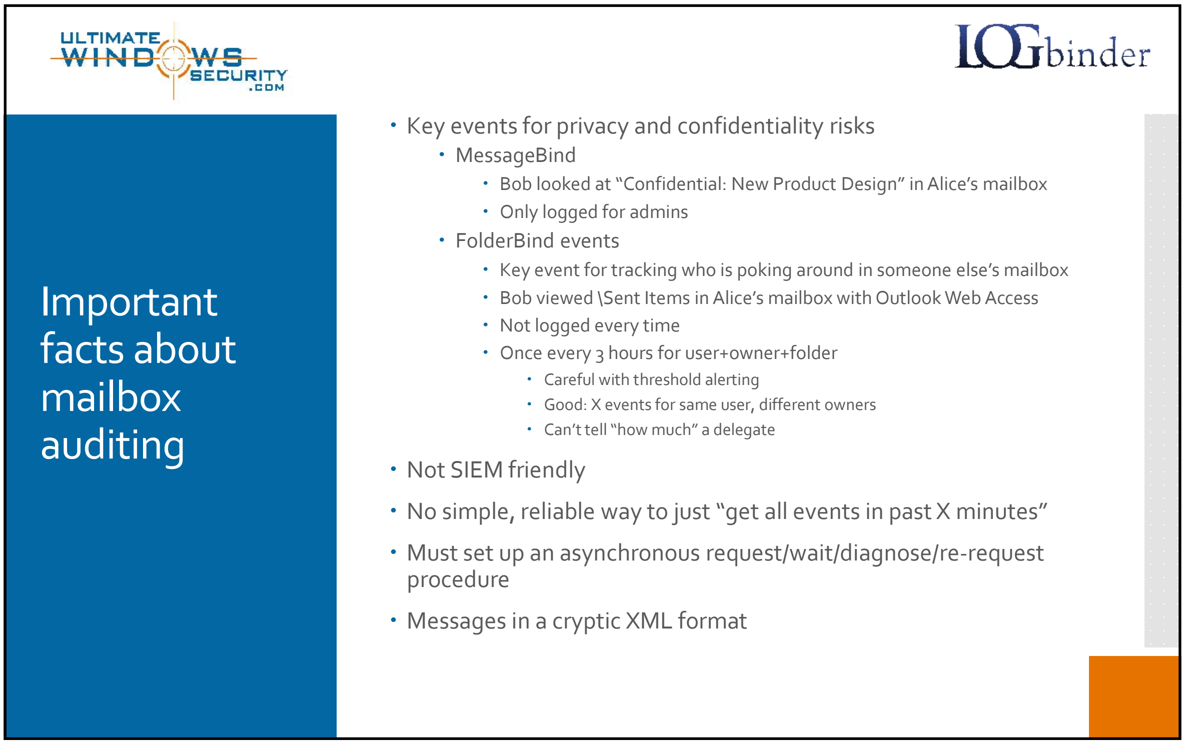
Exchange privileged user

- Reports in Exchange Admin Console



How do you access the audit log?

- PowerShell commands
  - To get all events for all mailboxes
    - Issue periodic asynchronous PowerShell commands
      - New-MailboxAuditLogSearch
    - Wait for Exchange to email you results in XML file
    - What can happen
      - Email never arrives
      - Error email: results too large
  - Otherwise, request audit events for specified –Identity
    - Search-MailboxAuditLog –Identity "Marissa Myer"


ULTIMATE WINDOWS SECURITY .COM
LOGbinder

Important facts about mailbox auditing

- Key events for privacy and confidentiality risks
  - MessageBind
    - Bob looked at "Confidential: New Product Design" in Alice's mailbox
    - Only logged for admins
  - FolderBind events
    - Key event for tracking who is poking around in someone else's mailbox
    - Bob viewed \Sent Items in Alice's mailbox with Outlook Web Access
    - Not logged every time
    - Once every 3 hours for user+owner+folder
      - Careful with threshold alerting
      - Good: X events for same user, different owners
      - Can't tell "how much" a delegate
- Not SIEM friendly
- No simple, reliable way to just "get all events in past X minutes"
- Must set up an asynchronous request/wait/diagnose/re-request procedure
- Messages in a cryptic XML format

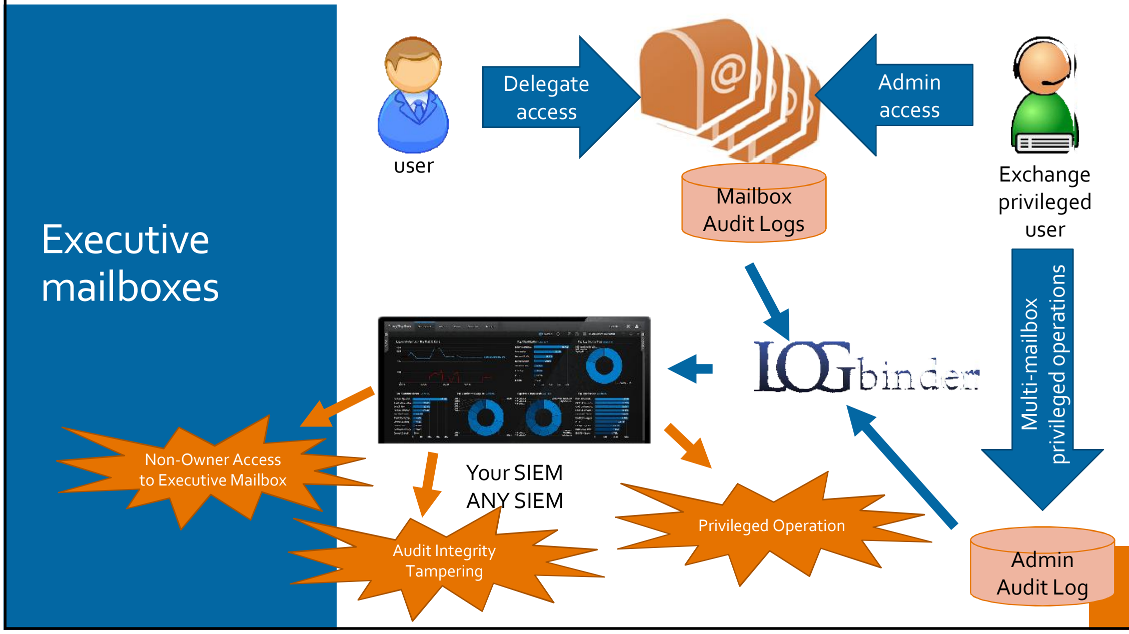
Important facts about mailbox auditing

- Many organizations want to focus on Exchange mailbox audit log and do not see Exchange **admin audit log** as a requirement
  - Unless you are only worried about delegate end-users
  - Do not care about privileged access to mailboxes
- That is a mistake
- Multitude of privileged operations that allow mailbox theft
- Only caught by the admin audit log
  - https://www.ultimatewindowssecurity.com/exchange/adminaudit/default.aspx

Fulfilling enterprise compliance and security requirements

- Auditing must be enabled consistently o mailboxes in a timely manner
- Audit logs must be quickly collected to secure archive
  - Otherwise no accountability or integrity
- Security operations team needs to correlat activity across entire enterprise
  - SIEM needs all security logs
- When executive mailboxes are accessed by non-owners
  - Security team needs to know NOW
- When audit logs or audit policy is tampered with
  - Security team needs to know NOW

Executive mailboxes



user

Delegate access

Admin access

Mailbox Audit Logs

Exchange privileged user

Multi-mailbox privileged operations

LOGbinder

Your SIEM
ANY SIEM

Non-Owner Access to Executive Mailbox

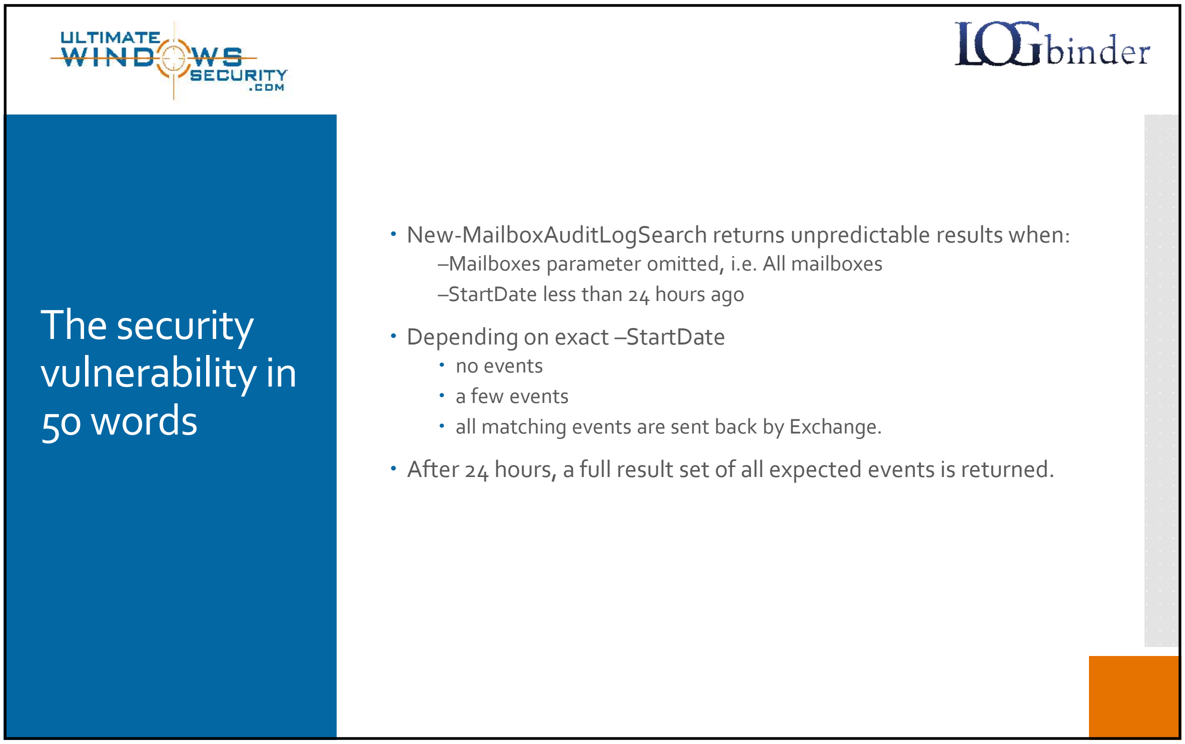
Audit Integrity Tampering

Privileged Operation

Admin Audit Log

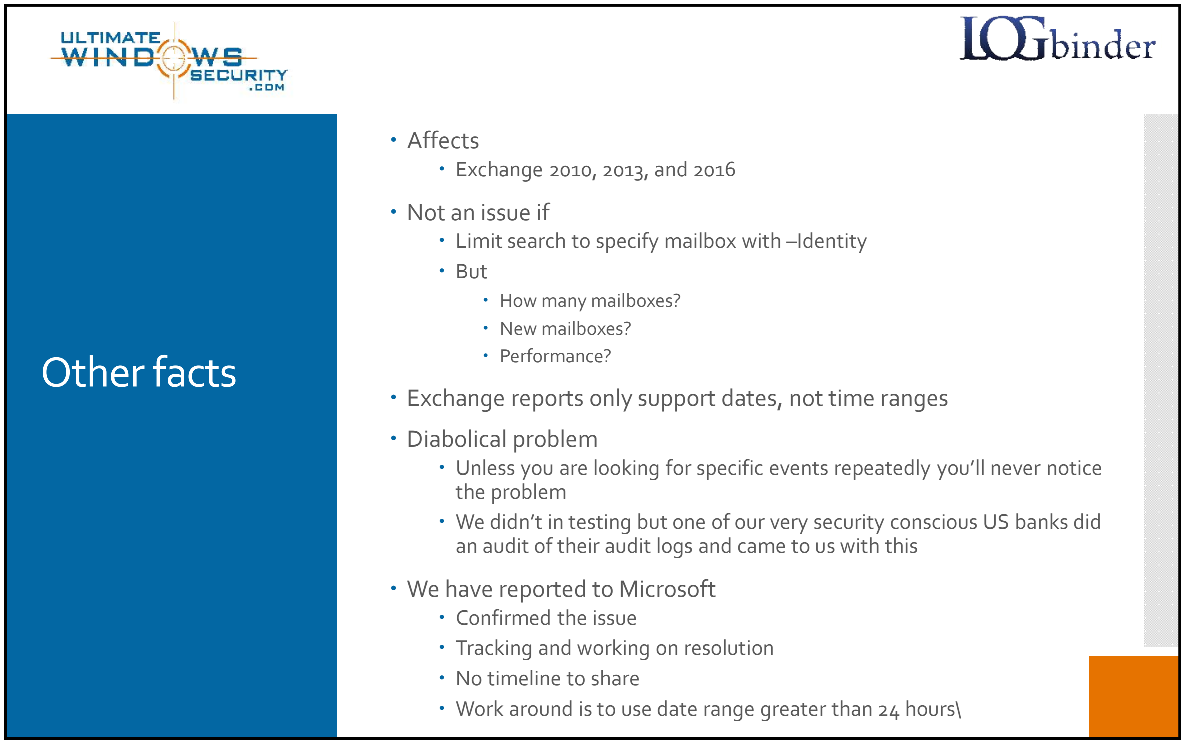
LOGbinder

- 5 minute install on any VM in domain
- Nothing installed on Exchange servers
- Supports least privilege
- Content packs for many SIEMs



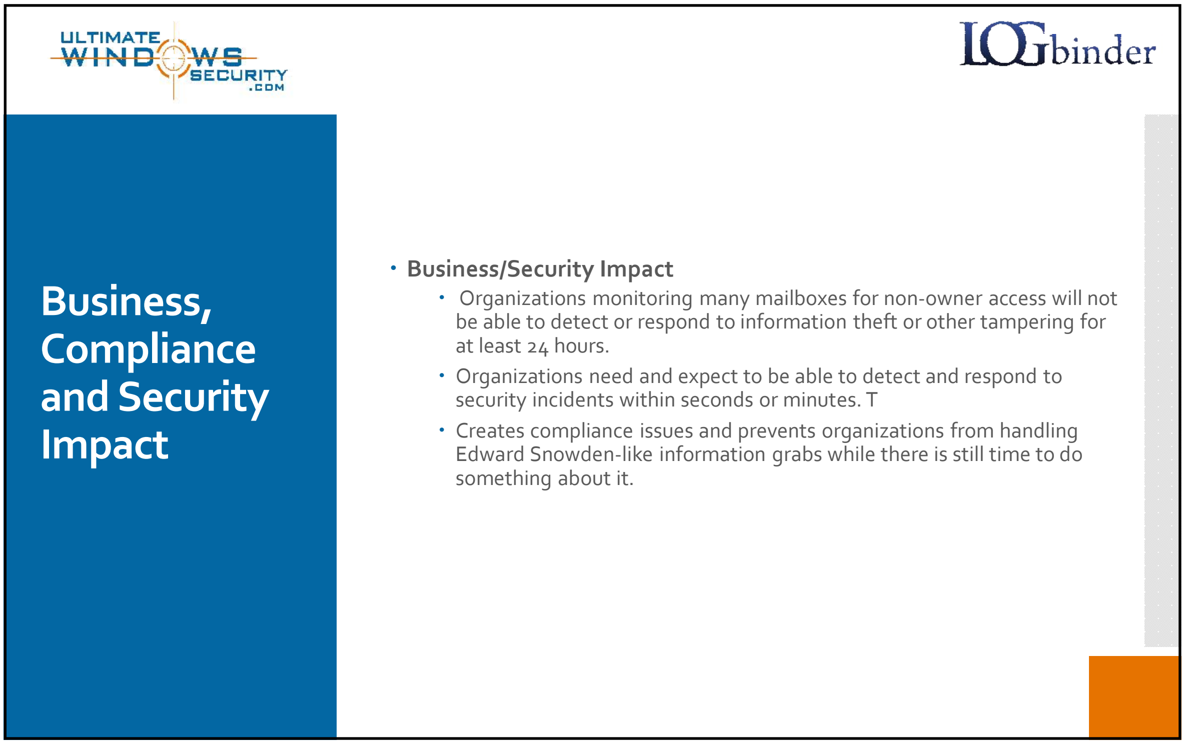
The security vulnerability in 50 words

- New-MailboxAuditLogSearch returns unpredictable results when:
  - –Mailboxes parameter omitted, i.e. All mailboxes
  - –StartDate less than 24 hours ago
- Depending on exact –StartDate
  - no events
  - a few events
  - all matching events are sent back by Exchange.
- After 24 hours, a full result set of all expected events is returned.



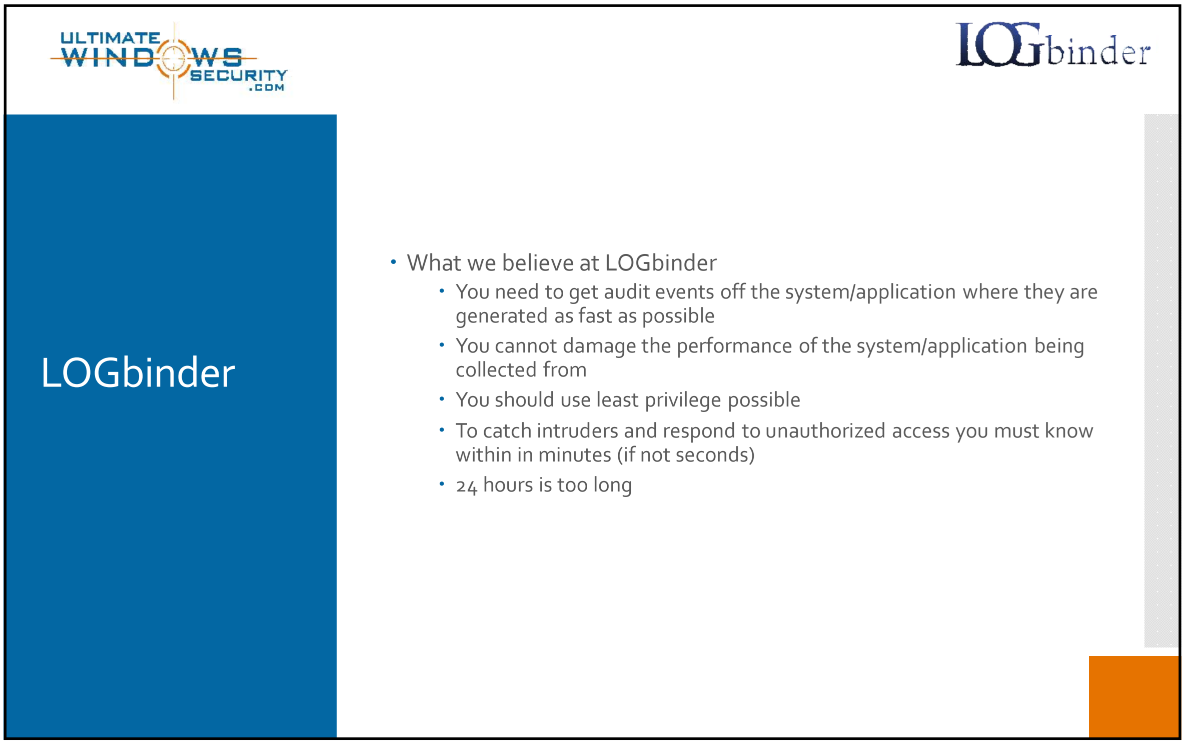
Other facts

- Affects
  - Exchange 2010, 2013, and 2016
- Not an issue if
  - Limit search to specify mailbox with –Identity
  - But
    - How many mailboxes?
    - New mailboxes?
    - Performance?
- Exchange reports only support dates, not time ranges
- Diabolical problem
  - Unless you are looking for specific events repeatedly you'll never notice the problem
  - We didn't in testing but one of our very security conscious US banks did an audit of their audit logs and came to us with this
- We have reported to Microsoft
  - Confirmed the issue
  - Tracking and working on resolution
  - No timeline to share
  - Work around is to use date range greater than 24 hours\



Business, Compliance and Security Impact

- **Business/Security Impact**
  - Organizations monitoring many mailboxes for non-owner access will not be able to detect or respond to information theft or other tampering for at least 24 hours.
  - Organizations need and expect to be able to detect and respond to security incidents within seconds or minutes. T
  - Creates compliance issues and prevents organizations from handling Edward Snowden-like information grabs while there is still time to do something about it.

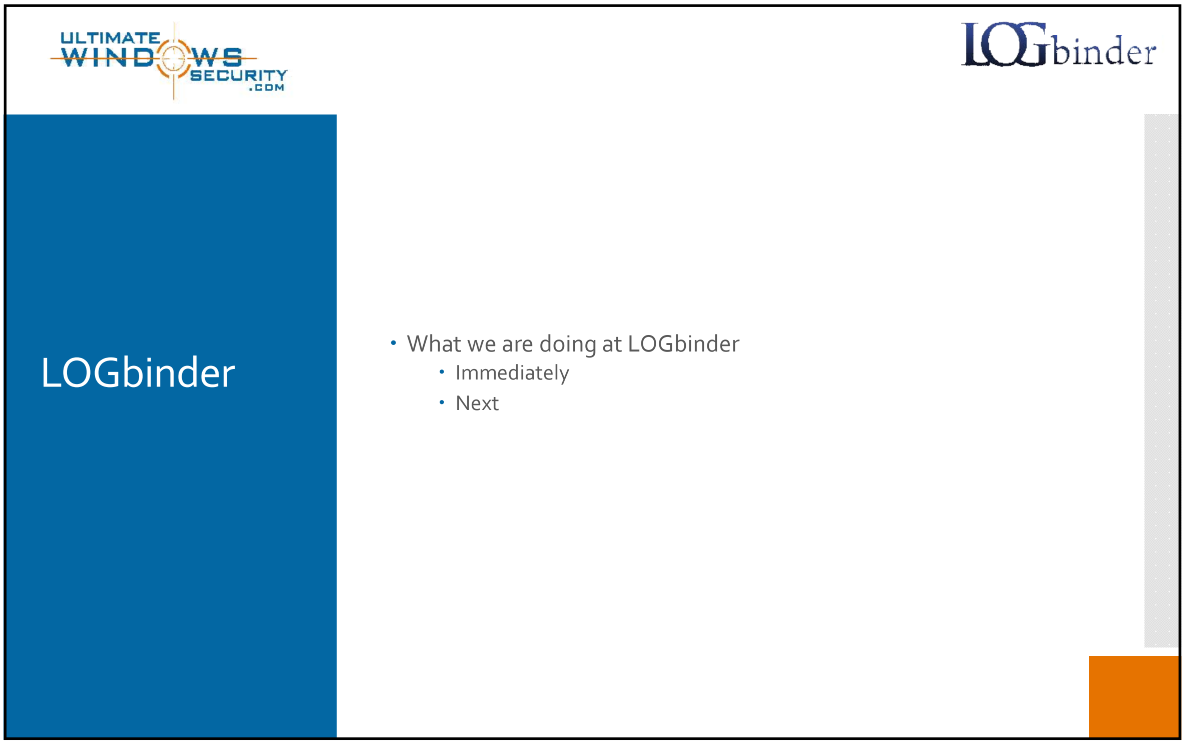


LOGbinder

- What we believe at LOGbinder
  - You need to get audit events off the system/application where they are generated as fast as possible
  - You cannot damage the performance of the system/application being collected from
  - You should use least privilege possible
  - To catch intruders and respond to unauthorized access you must know within in minutes (if not seconds)
  - 24 hours is too long

LOGbinder

- What we are doing at LOGbinder
  - Immediately
  - Next



LOGbinder

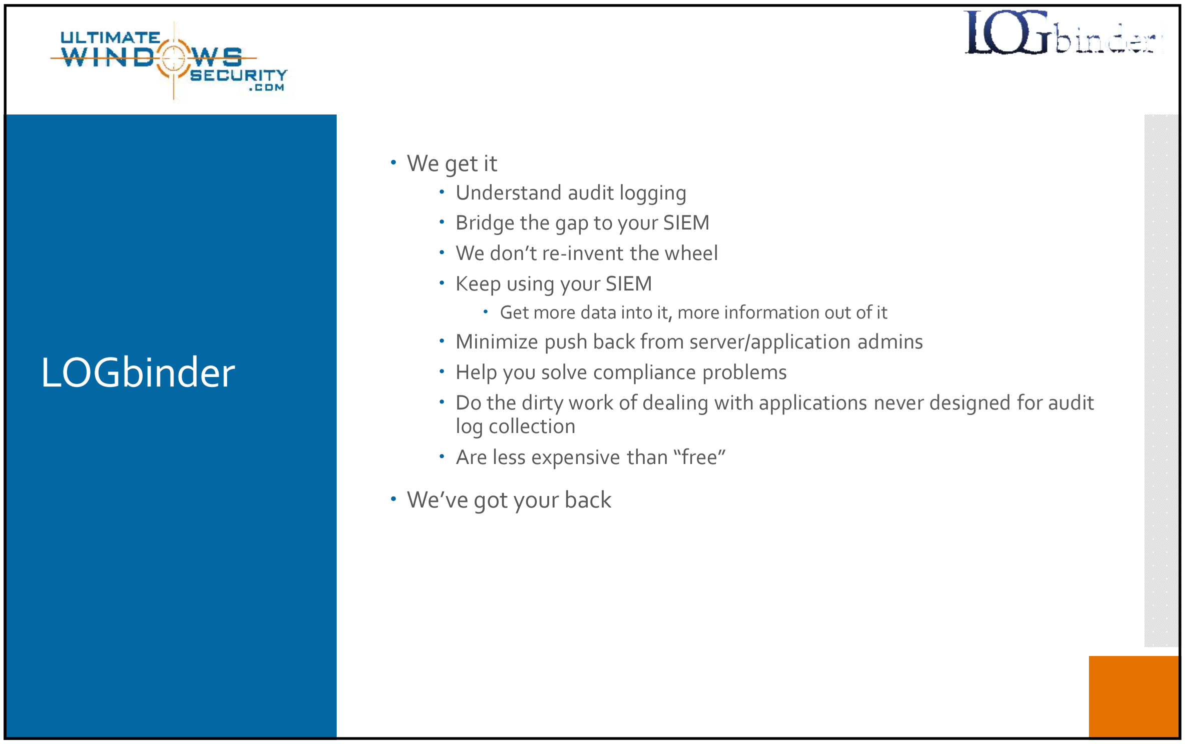
- What we are doing at LOGbinder
  - Immediately
  - Next

Immediately

- LOGbinder for Exchange 3.1
  - Optional 24 hour delay for mailbox audit log collection

Next

- New feature: Targeted, Synchronous Mailbox Audit Log Collection
- You specify groups or OUs of executives or other sensitive mailboxes
- LOGbinder uses synchronous mailbox audit log searches on those groups and OUs
- Non-targeted mailbox audit logs collected 24 hours later
  - No duplication of events
- Benefits
  - Compensating control for 24 hour Exchange bug
    - Important for compliance
  - Targeted mailbox audit events reach your SIEM faster than ever
    - Thanks to synchronous collection
    - Benefit even if and when Microsoft fixes bug
- Request beta from zself@logbinder.com



LOGbinder

- We get it
  - Understand audit logging
  - Bridge the gap to your SIEM
  - We don't re-invent the wheel
  - Keep using your SIEM
    - Get more data into it, more information out of it
  - Minimize push back from server/application admins
  - Help you solve compliance problems
  - Do the dirty work of dealing with applications never designed for audit log collection
  - Are less expensive than "free"
- We've got your back