RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

MATTERS NOW

SESSION ID: CSV-F03

OFFICE 365 SECURITY: TOP PRIORITIES FOR 30 DAYS, 90 DAYS AND BEYOND

Mark Simos

Lead Cybersecurity Architect
Microsoft
@MarkSimos

Matt Kemelhar

Global Director, Incident Response
Microsoft

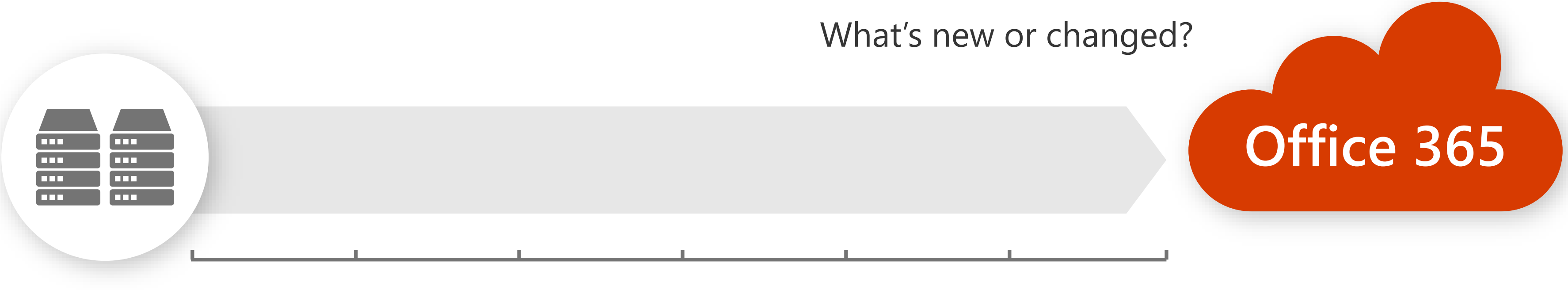
Session Outline

1. LIFE ON THE CLOUD (AS SECURITY)

What is security like when fully on Office 365?

What's gone?

What's new or changed?



2. THE JOURNEY

How do I get the most for my security investments?

1. LIFE ON THE CLOUD (AS SECURITY)

What is security like when fully on Office 365?

What’s gone?

What’s new or changed?

Office 365

Responsibility Zones

Responsibility	SaaS	PaaS	IaaS	On-prem	
Data governance and rights management	🟦	🟦	🟦	🟦	Always retained by customer
Client endpoints	🟦	🟦	🟦	🟦	
Account and access management	🟦	🟦	🟦	🟦	
Identity and directory infrastructure	◥	◥	🟦	🟦	Varies by service type
Application	⬜	◥	🟦	🟦	
Network controls	⬜	◥	🟦	🟦	
Operating system	⬜	⬜	🟦	🟦	
Physical hosts	⬜	⬜	⬜	🟦	Transfers to Cloud Provider
Physical network	⬜	⬜	⬜	🟦	
Physical datacenter	⬜	⬜	⬜	🟦	

⬜ Microsoft 🟦 Customer

Security Responsibilities Transfer to Office 365

Responsibility	SaaS
Data governance and rights management	🟦
Client endpoints	🟦
Account and access management	🟦
Identity and directory infrastructure	◩
Application	⬜
Network controls	⬜
Operating system	⬜
Physical hosts	⬜
Physical network	⬜
Physical datacenter	⬜

Security Patches (Server)

Feature Upgrades*

Service Uptime
→ SLA from Microsoft

Server Maintenance and Troubleshooting

Backup and Archive

Attacks on

- Operating System (OS) and Admins
- Application attacks
- Hardware/Firmware

Denial of Service

Physical Attacks

⬜ Microsoft 🟦 Customer

**You still need to manage feature configuration*

Key Change

Responsibility	SaaS
Data governance and rights management	🟦
Client endpoints	🟦
Account and access management	🟦
Identity and directory infrastructure	◪
Application	⬜
Network controls	⬜
Operating system	⬜
Physical hosts	⬜
Physical network	⬜
Physical datacenter	⬜

⬜ Microsoft 🟦 Customer

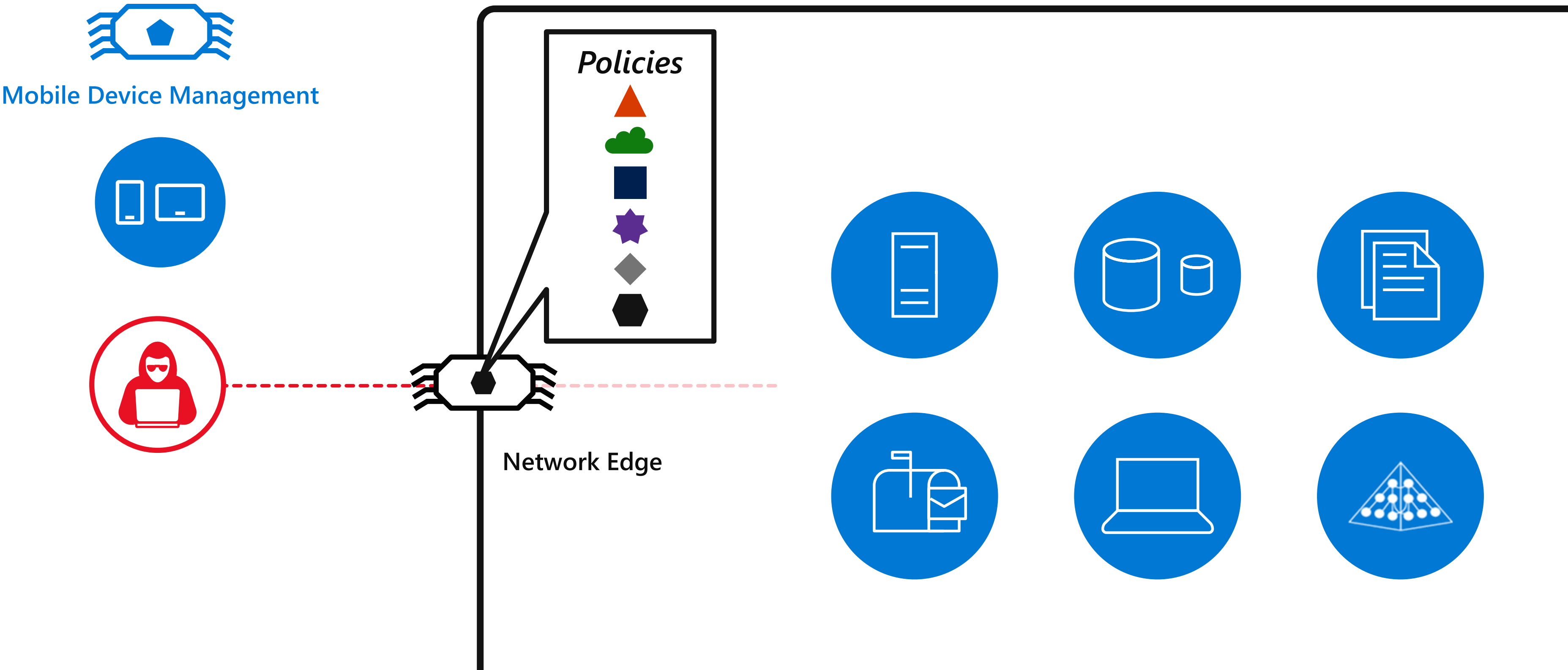
“No Firewall”

Service connected directly to Internet (users and ***admin interfaces***)

Implications

1. **Authentication Security is *Extremely Critical***
   - Multi-factor authentication
   - Anomaly detection using
   - User and Entity **Behavior** Analytics (UEBA)
   - **Context** awareness (time, date, geolocation)
   - Integrated security **intelligence**
2. **Tenant Security Configuration is Critical**

Evolution of Visibility and Policy Enforcement

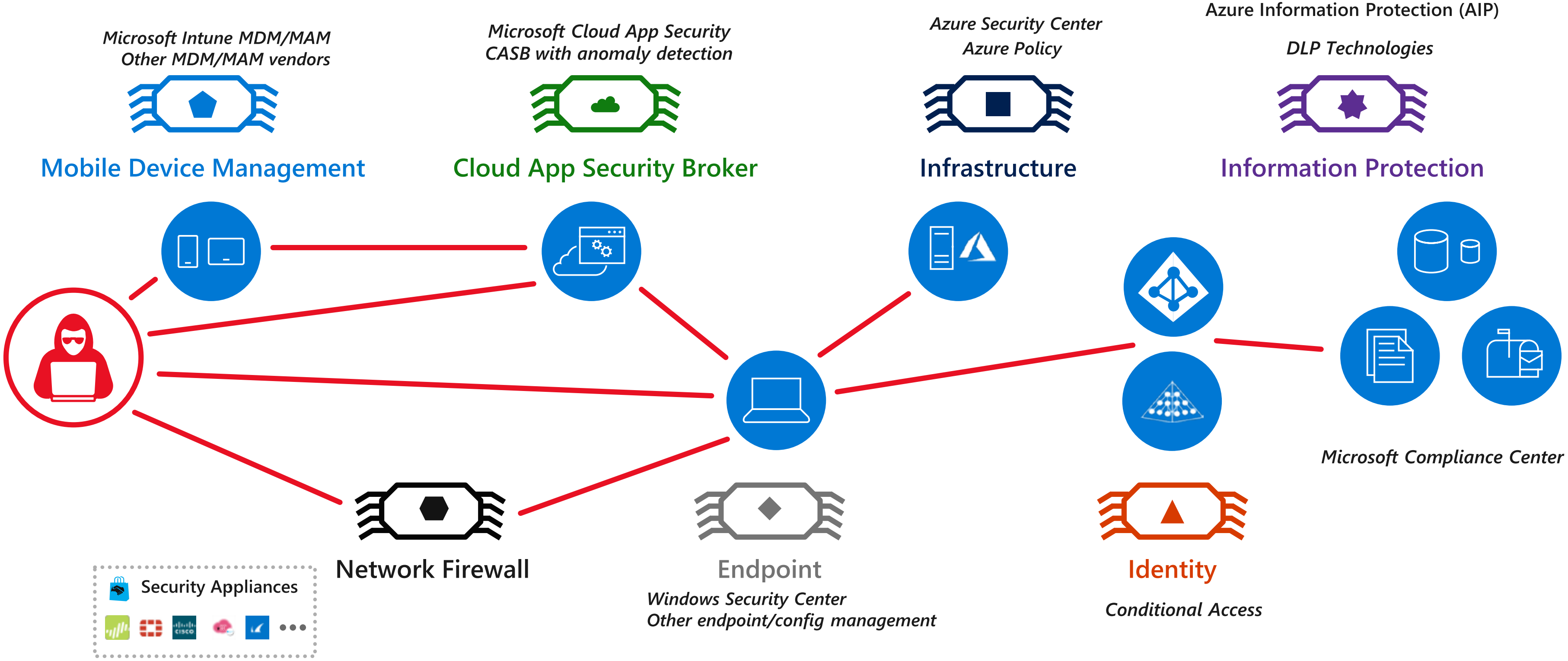


Mobile Device Management

Policies

Network Edge

Evolution of Visibility and Policy Enforcement



Microsoft Intune MDM/MAM
Other MDM/MAM vendors

Mobile Device Management

Microsoft Cloud App Security
CASB with anomaly detection

Cloud App Security Broker

Azure Security Center
Azure Policy

Infrastructure

Azure Information Protection (AIP)

DLP Technologies

Information Protection

Microsoft Compliance Center

Security Appliances

Network Firewall

Endpoint

Windows Security Center
Other endpoint/config management

Identity

Conditional Access

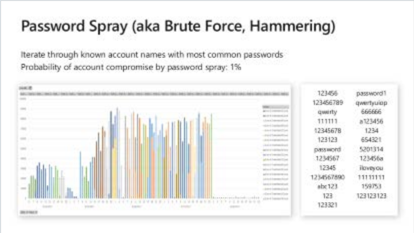
Must shift to policy and controls tailored for each asset type

Responsibility	SaaS
Data governance and rights management	🟦
Client endpoints	🟦
Account and access management	🟦
Identity and directory infrastructure	◩
Application	⬜
Network controls	⬜
Operating system	⬜
Physical hosts	⬜
Physical network	⬜
Physical datacenter	⬜

Threats change a bit...

Notable trends:

1. Identity Attacks
   - Password spray
   - Brute force
   - Password re-use
2. App/Data Layer Attacks
   - Social engineering
   - Delegation and forwarding rule attacks
   - PowerShell scripts in attacks



Password Spray (aka Brute Force, Hammering)

Iterate through known account names with most common passwords
Probability of account compromise by password spray: 1%

123456
123456789
qwerty
111111
12345678
123123
password
1234567
12345
1234567890
abc123
123
123321

password1
qwertyuiop
666666
a123456
1234
654321
5201314
123456a
iloveyou
11111111
159753
123123123

For more information, see https://aka.ms/O365attacks

1. LIFE ON THE CLOUD (AS SECURITY)

What is security like when fully on Office 365?

What's gone?

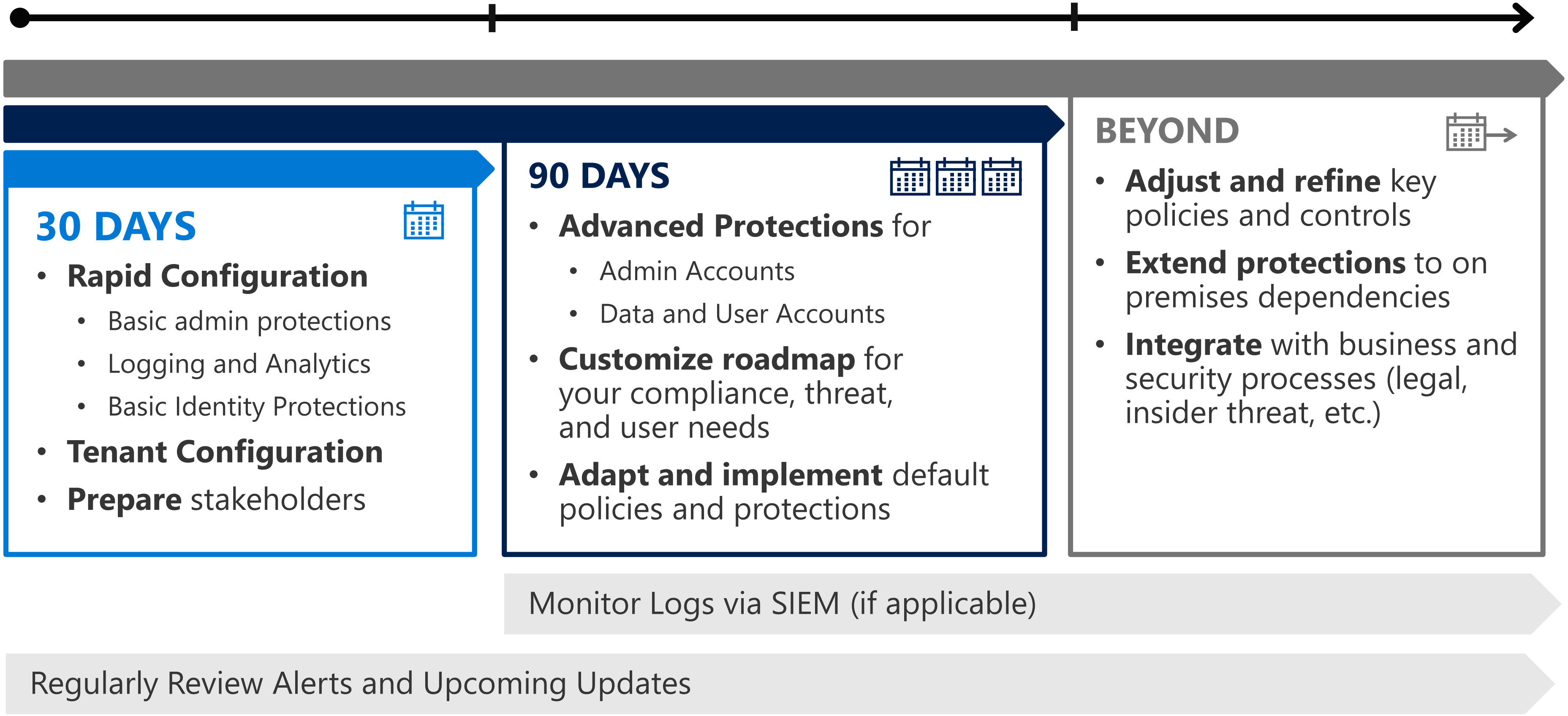
What's new or changed?

2. THE JOURNEY

How do I get the most for my security investments?

Roadmap Outcomes

How do I quickly and efficiently protect my Office 365 Tenant?



30 DAYS

- **Rapid Configuration**
  - Basic admin protections
  - Logging and Analytics
  - Basic Identity Protections
- **Tenant Configuration**
- **Prepare** stakeholders

90 DAYS

- **Advanced Protections** for
  - Admin Accounts
  - Data and User Accounts
- **Customize roadmap** for your compliance, threat, and user needs
- **Adapt and implement** default policies and protections

BEYOND

- **Adjust and refine** key policies and controls
- **Extend protections** to on premises dependencies
- **Integrate** with business and security processes (legal, insider threat, etc.)

Monitor Logs via SIEM (if applicable)

Regularly Review Alerts and Upcoming Updates

30 DAY Plan

THREAT PROTECTION

Admins

- Separate Admin Account
- Enforce MFA for admins
- Highly Secure Productivity Device

Windows 10 example http://aka.ms/HighSecWin10

Tenant / All Users

- Enable logging + anomaly detection (Example: Microsoft Cloud App Security)

INFORMATION PROTECTION

○ Evaluate example Information Protection policies https://aka.ms/O365DataPolicy

○ = Start preparation for action in 90 day plan

IDENTITY AND ACCESS MANAGEMENT

- Enable Azure AD Identity protection

  Ensure passwords are synchronized to Azure AD

- If Federated, enforce account security (Password length / age / complexity, etc.)

○ Evaluate example conditional access policies https://aka.ms/O365IdentityPolicy

SECURITY MANAGEMENT

Configure Roles, Policies, Email/Collaboration Protection, tenant security settings, and Cloud App Security Broker (CASB) – https://aka.ms/O365TenantSecurity

Regularly Review Alerts (CASB, Threat Dashboard) and Upcoming Changes (Roadmap | Blog | YouTube)

90 DAY Plan

THREAT PROTECTION

Admins

- Privileged Access Workstation http://aka.ms/cyberpaw
- Configure Azure AD PIM

Tenant / All Users

- Configure SIEM to collect logs from Federation, CASB, and Office 365

INFORMATION PROTECTION

- **Adapt and Implement** Information Protection policies https://aka.ms/O365DataPolicy

IDENTITY AND ACCESS MANAGEMENT

- Enable and Enforce **Multi-factor Authentication** for all users
- **Adapt and Implement** Conditional Access policies https://aka.ms/O365IdentityPolicy

SECURITY MANAGEMENT

Plan actions for your unique security needs using:

- **Secure Score** – Identify important actions and low hanging fruit https://securescore.microsoft.com
- **Sharing Risks** – Use CASB to identify oversharing of sensitive/internal documents
- **Threat Intelligence** – Conduct Attack Simulation + Industry Trends
- **Compliance Status** – Compliance manager (GDPR, NIST 800-171) https://servicetrust.microsoft.com/ComplianceManager

Regularly Review Alerts (CASB, Threat Dashboard, SIEM) and Upcoming Updates

...And BEYOND

THREAT PROTECTION

Admins

- SPA roadmap for on premises AD http://aka.ms/SPAroadmap

Tenant / All Users

- Integrate Cloud App Security Broker (CASB) into
  - Insider threat program
  - Shadow IT GRC risks/program

INFORMATION PROTECTION

- Integrate AIP into insider threat risk strategy
- Refine Information Protection policies
  - Office 365 DLP
  - CASB policies and alerts
  - Data Encryption Solution

IDENTITY AND ACCESS MANAGEMENT

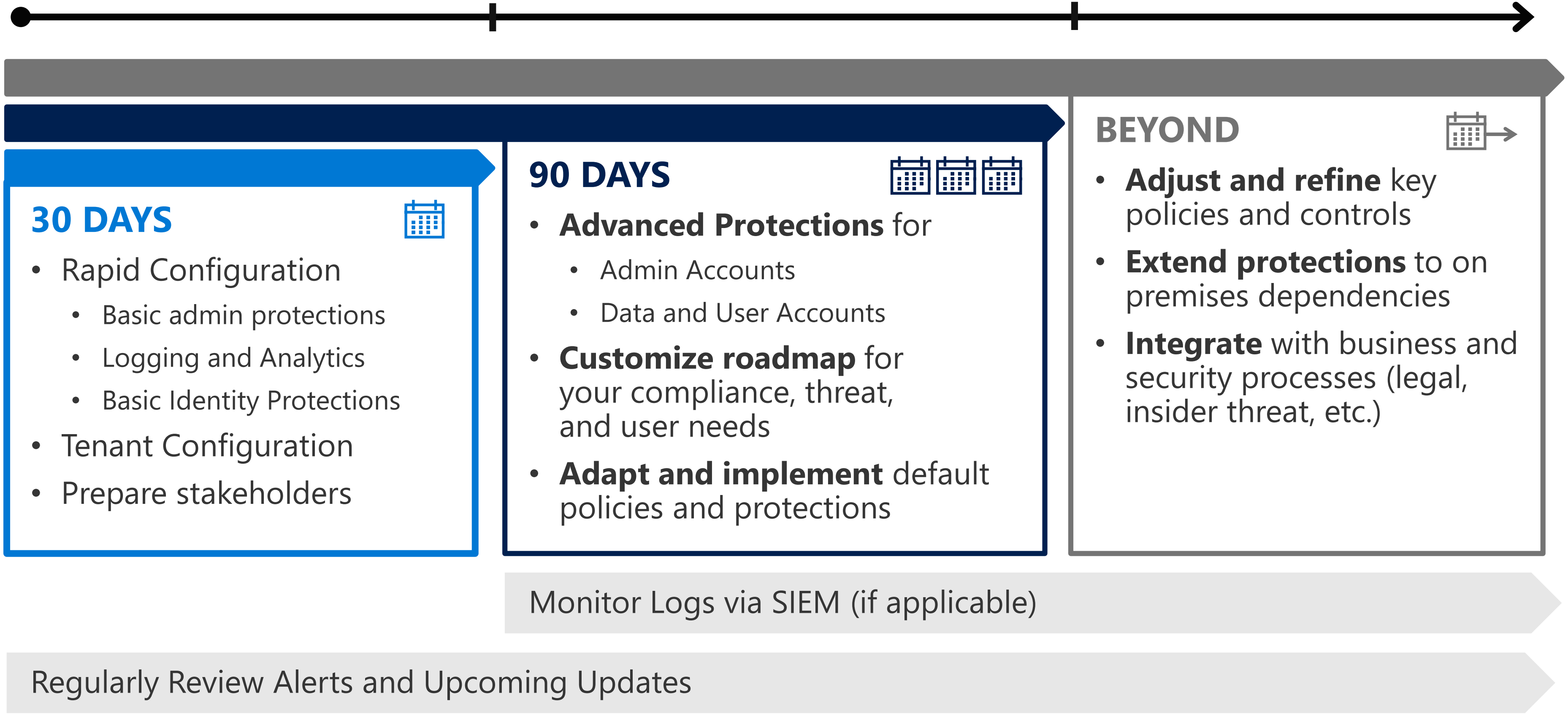
- Refine policies and operational process
- Integrate alerts on user behavior in with insider threat program (from Azure AD Identity Protection or other capability)

SECURITY MANAGEMENT

- **Secure Score** – Continue Planning Next Actions
- **eDiscovery** – Integrate into legal and threat response processes

Regularly Review Alerts and Upcoming Updates

Questions?



30 DAYS

- Rapid Configuration
  - Basic admin protections
  - Logging and Analytics
  - Basic Identity Protections
- Tenant Configuration
- Prepare stakeholders

90 DAYS

- **Advanced Protections** for
  - Admin Accounts
  - Data and User Accounts
- **Customize roadmap** for your compliance, threat, and user needs
- **Adapt and implement** default policies and protections

BEYOND

- **Adjust and refine** key policies and controls
- **Extend protections** to on premises dependencies
- **Integrate** with business and security processes (legal, insider threat, etc.)

Monitor Logs via SIEM (if applicable)

Regularly Review Alerts and Upcoming Updates

Microsoft

Thank you

@MarkSimos

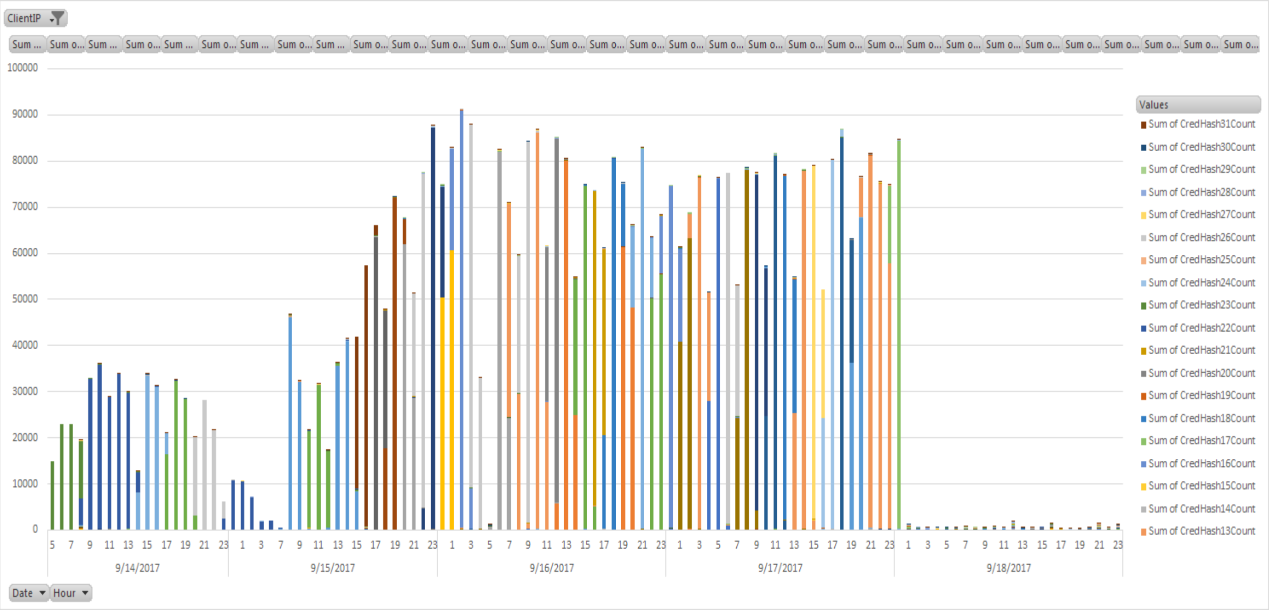
https://aka.ms/markslist

REFERENCES

Password Spray (aka Brute Force, Hammering)

Iterate through known account names with most common passwords

Probability of account compromise by password spray: 1%



123456
123456789
qwerty
111111
12345678
123123
password
1234567
12345
1234567890
abc123
123
123321

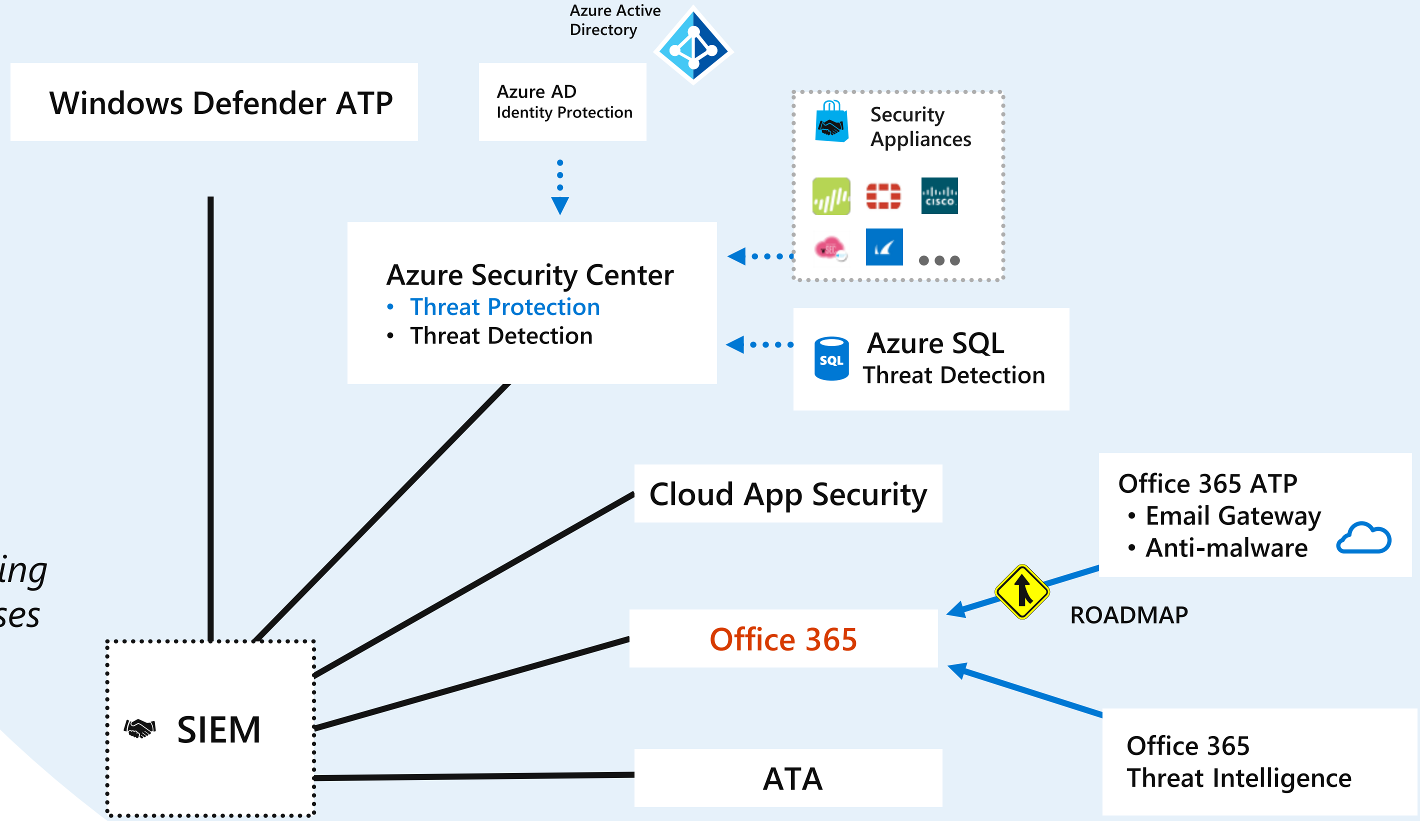
password1
qwertyuiop
666666
a123456
1234
654321
5201314
123456a
iloveyou
11111111
159753
123123123

References

- **Office 365 Updates**
  Office 365 Roadmap | O365 Update Series on YouTube
- **Office 365 Secure Score**
  https://securescore.office.com/
- **Office 365 Security Reference Configuration**
  http://aka.ms/securecampaign
- **Securing Privileged Access Roadmap**
  http://aka.ms/sparoadmap
- **Deploy Privileged Access Workstations**
  http://aka.ms/cyberpaw
- **Standards for a Highly Secure Windows 10 Device**
  http://aka.ms/HighSecWin10
- **Cloud App Security**
  https://docs.microsoft.com/en-us/cloud-app-security/connect-office-365-to-microsoft-cloud-app-security
- **Enable Azure AD Identity Protection**
  https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection-enable

Integrating with your SIEM

Powered by the Intelligent Security Graph



Azure Active Directory

Windows Defender ATP

Azure AD Identity Protection

Security Appliances

Azure Security Center
- Threat Protection
- Threat Detection

Azure SQL Threat Detection

Cloud App Security

Office 365 ATP
- Email Gateway
- Anti-malware

ROADMAP

Office 365

Office 365 Threat Intelligence

SIEM

ATA

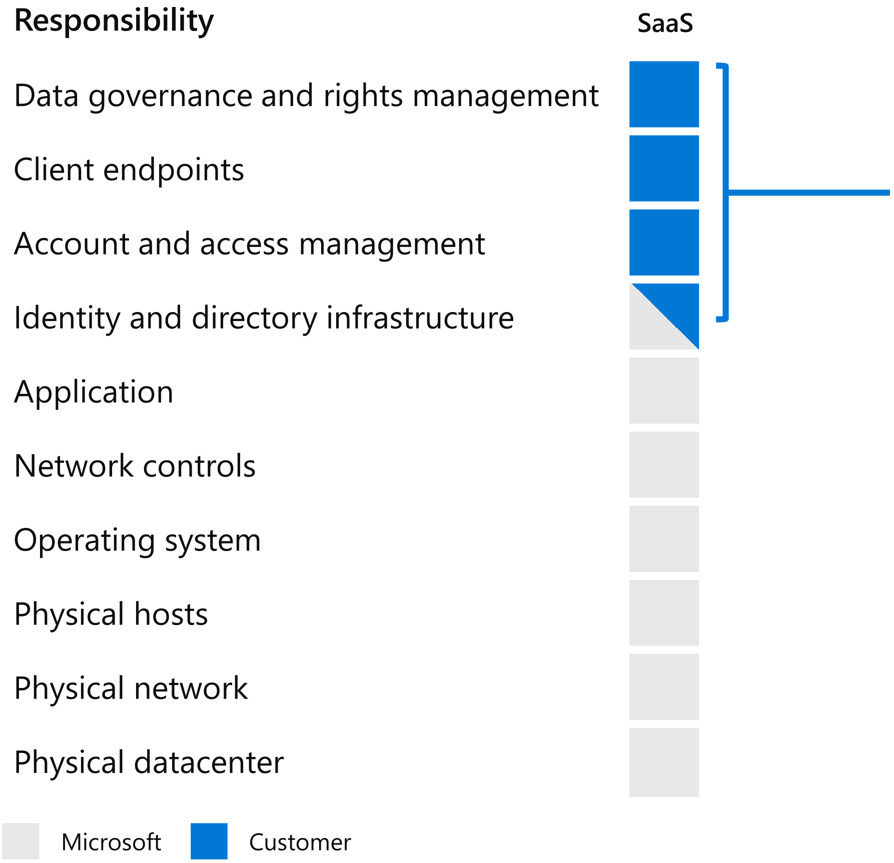
Connect to your existing SIEM tool and processes

— Log Integration
← Audit Logs
⇠ Alerts

SIEM Integration Reference

- **Windows Defender ATP**
  https://technet.microsoft.com/en-us/itpro/windows/keep-secure/enable-siem-integration-windows-defender-advanced-threat-protection
- **Advanced Threat Analytics**
  https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/configure-event-collection
  https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/setting-ata-alerts
- **Azure SIEM Integration (includes Azure AD)**
  https://aka.ms/azureSIEMintegration
- **Office 365**
  https://support.office.com/en-us/article/Integrate-your-SIEM-server-with-Office-365-Cloud-App-Security-dd6d2417-49c4-4de6-9294-67fdabbf8532
- **Cloud App Security**
  https://docs.microsoft.com/en-us/cloud-app-security/siem
- **Operations Management Suite (OMS)**
  https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-log-search-api
  https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-api-alerts

Other Notable Changes



Responsibility	**SaaS**
Data governance and rights management	🟦
Client endpoints	🟦
Account and access management	🟦
Identity and directory infrastructure	◪
Application	⬜
Network controls	⬜
Operating system	⬜
Physical hosts	⬜
Physical network	⬜
Physical datacenter	⬜

⬜ Microsoft 🟦 Customer

- PowerShell for administration (and attacks)
- Authentication flow changes (protocols, log locations, etc.)
- Log analytics easier/faster/better (with CASB anomaly detection + O365 Logs)

- Regular release of features/changes (configurable, but not customizable)

Implications

- Always Current Features
- Security must regularly review updates
  Office 365 Roadmap | O365 Update Series on YouTube

Security Log Notes

KEY LOG LOCATIONS

- Azure AD – Account Authentication/Management
- Office 365 Security and Compliance Center – O365 App Usage
- SIEM integration – See reference slide

THERE IS A DELAY FOR SOME LOGS (30-60 MINUTES)

ENABLING LOGS IN EXCHANGE

- Admin and Non-Owner Logging are on by default
- Owner Logging (e.g. activities in my mailbox) must be enabled
  - Secure Score can launch script to enable this
  - Cloud App Security needs this for some anomaly detection

Observed to increase risk of security incidents

PRIVILEGE HYGIENE

- Missing key protections for privileged accounts (see 30 day plan)
  - Includes accounts with powerful permissions (eDiscovery, HR/Compliance account)
- Multiple people sharing a single account/password
- Granting broad permissions to data (SharePoint/OneDrive)

TENANT CONFIGURATION

- Logging not enabled (hampers incident investigation)
- Weak password policies in on-premises AD (Federated Identity)
- Unused Security Capabilities (Advanced Threat Protection, Cloud App Security, etc.)

KEY STRATEGIC ELEMENT(S)

- Identify business critical data within O365
- SecureScore to measure risk exposure and progress
- Avoiding cloud features (e.g. avoiding password sync = not having leaked credential protection)