Microsoft 365

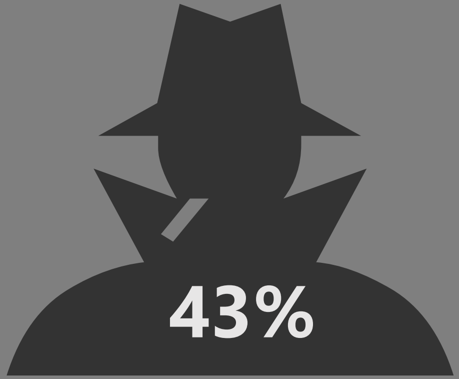
Security & Compliance
For Small- and Mid-Sized Businesses

Brandon Lecoq
Cybersecurity Manager

The reality for your business today, and the importance of proactive security

Cyberthreats are becoming more of a reality each day. 43% of cyber attacks target small business[1]. This disrupts how we live and work, how we acquire information and communicate, and what it takes to secure company data.

Providing peace of mind that your information and company data are safe is becoming a more important part of how we can work together.



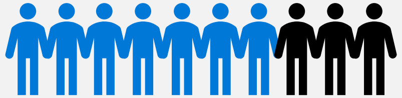
43% of cyber-attacks target small business[1]

[1] Small Business Trends, CYBER SECURITY STATISTICS – Numbers Small Businesses Need to Know, Jan. 3, 2017

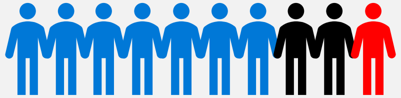
Cyberthreats by the numbers across 3 key attack zones

Email

Within 4 minutes



Open email from attacker



Will open attachment/link

286 days

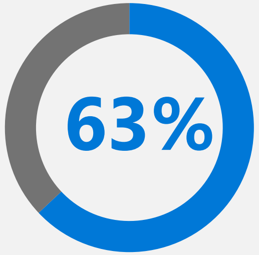
Detect intrusion

80 days

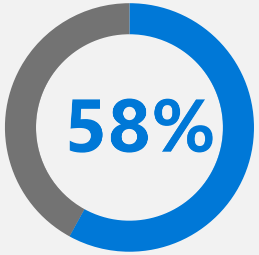
Contain damage

It takes hackers 4 min. to get into networks through email attacks and 286 days for detection, followed by an additional 80 days for damage control

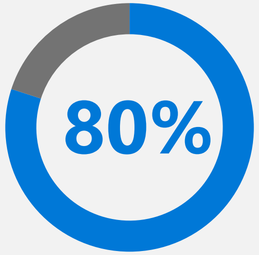
User



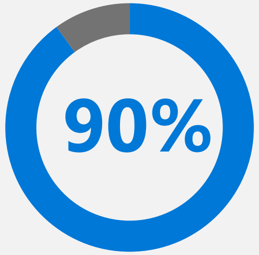
Weak, default, or stolen passwords



Accidently shares sensitive information



Non-approved SaaS usage: Shadow IT



Data leakage: 90% caused by user mistakes

Device

53 seconds

A laptop is stolen nearly every minute

55,000

Average devices compromised by Ransomware every month in 2016, 5X increase from 2015, 4X increase in Android base

200,000

PCs attacked by WannaCrypt across 150 countries

$1 Billion

Average earning of a hacker from Ransomware (FBI guesstimate)

Can you answer “Yes” to these 5 questions?

Do you **know** who is accessing your data?

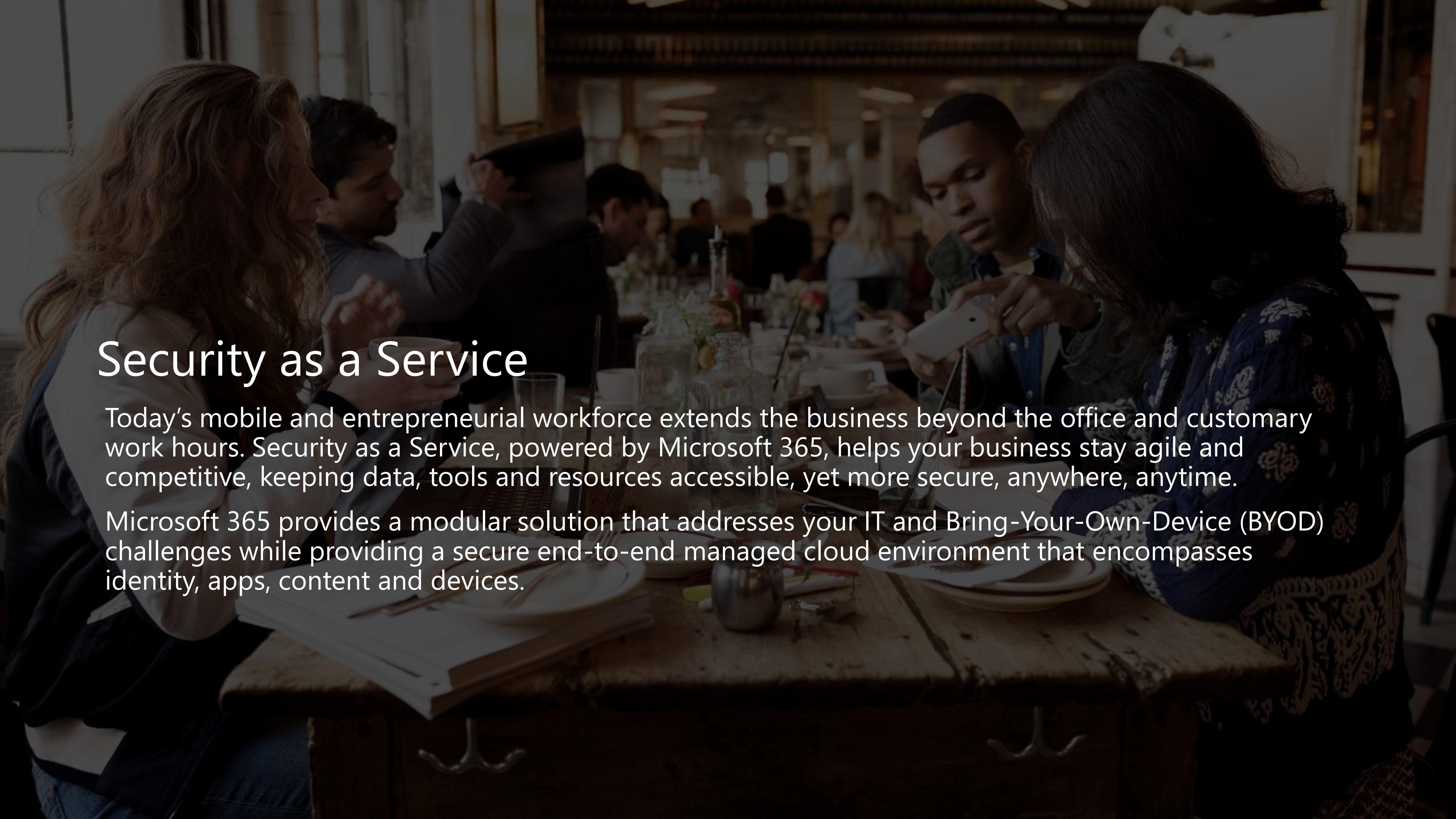
Can you **grant access** to your data based on risk in real time?

Can you quickly **find** and **react** to a breach?

Can you **protect** your data on devices, in the cloud, and in transit?

Do your users **love** their work experience?

If not, you may need Security as a Service



Security as a Service

Today’s mobile and entrepreneurial workforce extends the business beyond the office and customary work hours. Security as a Service, powered by Microsoft 365, helps your business stay agile and competitive, keeping data, tools and resources accessible, yet more secure, anywhere, anytime.

Microsoft 365 provides a modular solution that addresses your IT and Bring-Your-Own-Device (BYOD) challenges while providing a secure end-to-end managed cloud environment that encompasses identity, apps, content and devices.

Introducing Microsoft 365

We are living in a time of inflection. Digital transformation is the biggest change any of us has seen in our lifetime. Companies invest in technology to optimize operations, transform products, engage customers, and empower employees. The challenge is finding the way to empower people to do their best work. This starts with fostering a culture of work that is inspiring for everyone, and embraces the trends in the workplace that make work inspiring.

To deliver on the tremendous opportunity for business growth and innovation, we are simplifying the customer experience by bringing together Office 365, Windows 10, and Enterprise Mobility + Security with the introduction of Microsoft 365.

It's a complete, intelligent solution that empowers everyone to be creative and work together, securely.

Four core principles of Microsoft 365

Unlocks creativity

Built for teamwork

Integrated for simplicity

Intelligent security

Four key areas of **Intelligent Security**

Secure the front door

Protection from identity driven breaches, email attacks and attacks targeting OS

Secure content

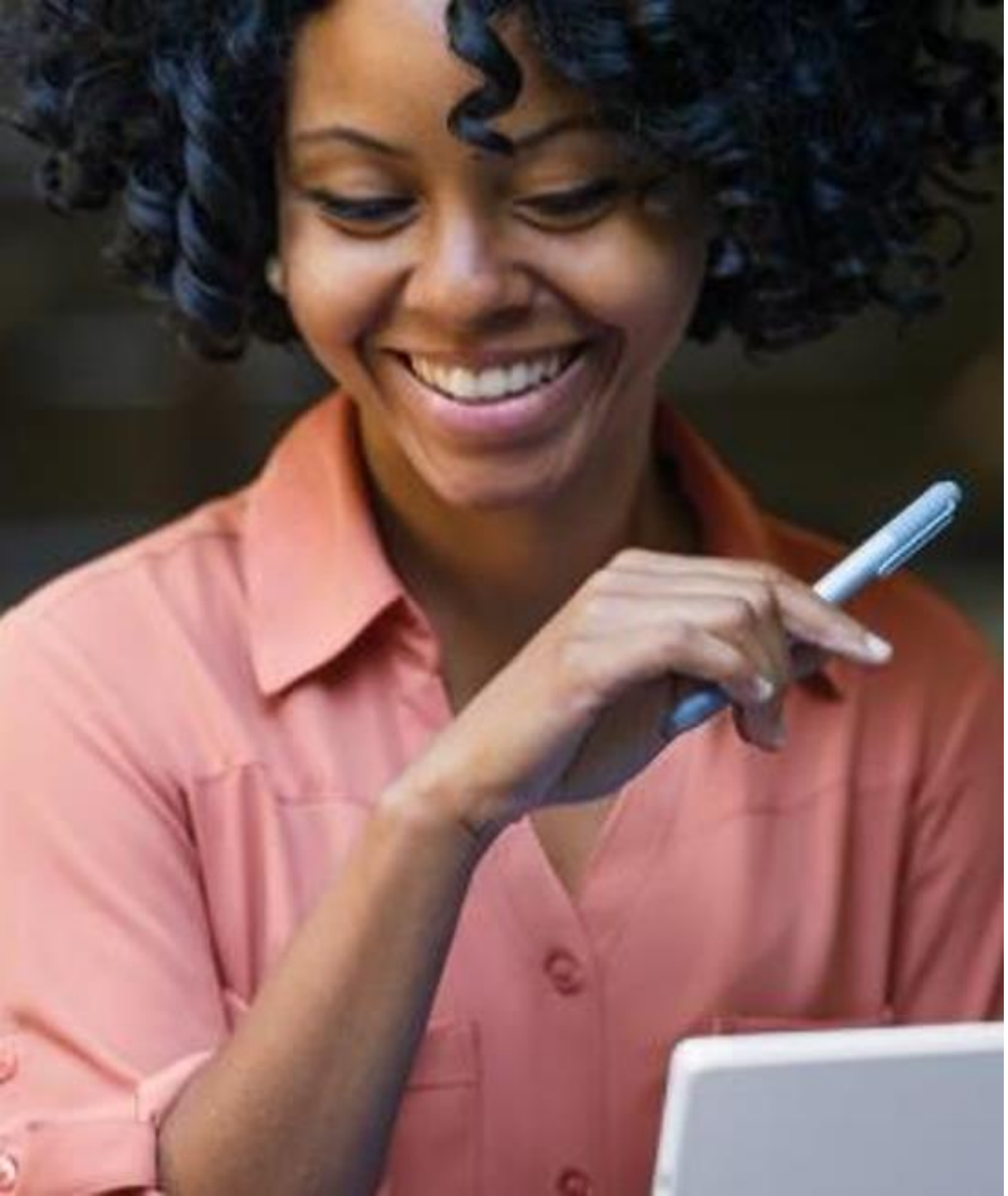
Protect content: At the time of creation, in transit, and during consumption

Secure devices

Workplace issued or BYOD devices

Great employee experience

Productivity without compromise



Secure the Front Door

Identity-Driven Security

Go beyond passwords and protect against identity compromise, while automatically identifying potential breaches before they cause damage.

- Risk-based Conditional Access and Multi-Factor Authentication
- Advanced security reporting
- Identify threats on-premises
- Identify high-risk usage of cloud apps, user behavior, detect abnormal downloads, prevent threats

Secure Content

Protect content: creation, transit, consumption

Use cloud applications without putting company information at risk by adding protection, ranging from access privileges to data encryption.

- Shadow IT Detection: Discovering Apps and Risk Scoring
- Intelligent Classification and Tagging of content
- Document encryption, tracking, revocation
- Monitoring shared files and responding to potential leaks
- Data segregation at a device/app level

Secure Devices

Workplace Issued or BYOD Devices

Manage company and BYOD devices to encrypt data and ensure compliance, automatically detect suspicious activities, and quickly block, quarantine, or wipe compromised devices.

- Conditional Access
- Device and App access level controls: PIN
- Device and App encryption at rest
- Save-As, Copy, Paste restrictions
- Device and App level data wipe

Great employee experience

Productivity without compromise

Implement tools and policies that empower your employees to be productive and secure on personal and company devices while maintaining control of data.

- Single Sign-On
- Self Service
- Advanced Multi-Factor Authentication
- App Proxy without the need of VPN

Which Microsoft 365 plan is right for you?

Choose the right Microsoft 365 plan for your organization's needs. Security add-ons can be used to tailor a solution that meets specific security and compliance requirements. To find the right starting point, review each of these scenarios:

DO YOU NEED…	Microsoft 365 Enterprise + ATP	Office 365 E3 + EMS E3 + ATP	Microsoft 365 Business + ATP
More than 100 seats?	●	●	
Extensive eDiscovery, data governance, and compliance tools?	●		
To protect highly sensitive data such as financial information, health records, or extensive IP?	●	●	
Real-time threat protection?	●	●	
Enterprise-level protection for cloud applications?	●	●	
On-premises domain controller?	●	●	
A solution that can be managed with little to no in-house IT staff?			●
Support for around 150 PCs?	●	●	
Does not need OS upgrade		●	
Needs Mobile Device Management and Mobile Application Management	●	●	
Low Risk Profile			●
Needs Proactive Attack Prevention on OS	●		

BEMO