Still Running 2016 Security in a 2026 Threat Landscape?

LeapFrog®

Still Running 2016 Security in a 2026 Threat Landscape?

Leapfrog Your Defenses Today

Small and midsize businesses (SMBs) face many of the same cybersecurity threats as large enterprises, but the way you prepare for and respond to those threats should be very different. Too often, security advice for SMBs is borrowed directly from enterprise playbooks. That advice typically adds layers of complexity to legacy systems like Classic Active Directory (AD): multiple admin accounts, password vault gymnastics, and policies that make day-to-day IT management harder and more expensive.

Leapfrog has over 25 years of experience helping SMBs grow by managing their IT and cybersecurity. Our Chief Technology Officer, Emmett Hawkins III, shares key trends he sees across the SMB landscape.

"The reality? You're not a large enterprise. You don't have 50-person IT departments or unlimited budgets. And while complexity might make sense at enterprise scale, for most businesses it creates friction, drives up costs, and still doesn't address the risks that actually matter most," Hawkins explains.

"The reality? You're not a large enterprise. You don't have 50-person IT departments or unlimited budgets. And while complexity might make sense at enterprise scale, for most businesses it creates friction, drives up costs, and still doesn't address the risks that actually matter most."

Where the Real Risks Are

Let's be clear about how most businesses are actually attacked today:

61% of businesses experienced a cyberattack in the past year (Verizon DBIR, 2024)

82% of ransomware victims are companies with fewer than 1,000 employees (Coveware, 2023)

$150,000–$250,000

is the average cost for SMB breach recovery (IBM, 2024)

Nearly all attacks begin remotely

via phishing emails, stolen credentials, or poorly secured remote access, not by someone physically accessing your network

The greatest risk to your business isn't whether your IT provider uses three admin accounts to reset a password. It's whether an attacker can trick an employee, steal their credentials, and use that access to move quickly through your systems.

Why the Status Quo Is Dangerous

Classic AD was built for a time when employees worked in offices, networks were trusted, and remote access was rare. Trying to patch and bolt on more controls to this outdated model is not only costly – it's risky.

There are countless point solutions that can be stitched together to make Classic AD slightly less vulnerable: password vaults, role segmentation, enhanced auditing, extra admin controls, and more. But in the end, you're left with a patchwork system that's expensive to maintain and still doesn't stop the attacks SMBs are most likely to face.

Put simply: the status quo leaves you exposed.

The greatest risk to your business isn't whether your IT provider uses three admin accounts to reset a password. It's whether an attacker can trick an employee, steal their credentials, and use that access to move quickly through your systems.

Where to Put Your Money

Instead of investing in complexity, focus on protections that block the attacks most likely to impact your business today:

- **Multi-Factor Authentication (MFA):** Blocks over 99% of credential-based attacks (Microsoft, 2023)
- **Email security and phishing defenses:** Over 90% of breaches start with phishing
- **Secure remote access:** Replace flat VPNs with modern gateways that verify users and devices
- **Endpoint Detection & Response (EDR):** Detects intrusions early before they spread
- **Active threat monitoring (SIEM/XDR/MDR):** Once reserved for large enterprises, continuous monitoring is now essential for all businesses

Leapfrog urges clients to take a proactive approach to cybersecurity. In addition to the above protections, we recommend investing in an Incident Response Plan to reduce the financial and reputational damage of a potential breach.

The Case for Modernization

Modern identity platforms like Microsoft Entra ID P2 offer:

- **Just-in-time privileges:** Admins receive elevated access only when needed, reducing risk
- **Built-in zero trust:** Every login and device must verify identity before access is granted
- **Cloud-first security:** Designed for remote work and SaaS environments

Pair this with Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA) to build a network that's both more secure and easier for employees to use. Instead of connecting to the entire network via VPN, employees access only the applications they need – no more, no less.

And remember: active threat monitoring (SIEM/XDR/MDR) is no longer optional. Attackers move fast. Automated alerts and managed detection ensure you know what's happening in real time – before a small compromise becomes a business disaster.

Attackers move fast. Automated alerts and managed detection ensure you know what's happening in real time – before a small compromise becomes a business disaster.

The Bottom Line

"Not all businesses are enterprises. You don't need enterprise-style complexity—you need focused investments that reduce real risk and enable modern work," Hawkins emphasizes.

- The threats you face are real and growing
- The status quo of Classic AD is dangerous
- Now is the time to modernize – to protect your business, your employees, and your future

At Leapfrog, our mission is to guide you through this transition. We help you prioritize investments, reduce unnecessary complexity, and adopt modern identity, Zero Trust, and active threat-monitoring capabilities that keep your business safe. We meet you where you are – and build strategic, scalable solutions for where you want to go.

Emmett Hawkins III *Chief Technology Officer, Leapfrog Services*

Emmett leads Leapfrog's technology strategy, service innovation, and hosted solutions, while advising clients as a trusted solutions architect. He co-founded Virtex Networks, one of the nation's first IT infrastructure service providers, acquired by Leapfrog in 2001. With deep expertise in enterprise management technologies, Emmett has held leadership roles at Computer Associates and served on advisory committees for the City of Atlanta. He is a member of InfraGard and a trustee of the Grace Scholarship Foundation. Emmett holds a BA from Emory University and is a graduate of Duke University's AMP program.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

Our managed IT services include:

Infrastructure Management
Security Management
Business Ops Management
Cybersecurity Solutions
IT Strategy & Consulting
C-Suite Services
Application Management
Support Services

Ready to leap ahead? If you're an SMB looking to modernize your cybersecurity and align with 2026 standards, Leapfrog is here to help. Our team specializes in simplifying complexity, reducing risk, and building secure, scalable solutions that support your growth.

Let's future-proof your business—reach out to us today.

@leapfrogservices | 404.870.2122 | www.LeapfrogServices.com | 1190 W. Druid Hills Dr., Ste. 200, Atlanta, GA 30329